YURA	ESG Management Policy	Num	YRC-24
		Modified date	2023.06.09
	Personal Data Protection Guidelines Policy	Page	0
		Department in charge	S&SHE Team

Notice

The ESG policy of Yura Corporation has been established based on the laws of the Republic of Korea, where the headquarters is located, and overseas subsidiaries operate in compliance with the headquarters' policy.

The key leadership of overseas subsidiaries aims to carry out their duties based on the laws of the Republic of Korea and the ESG policy of the headquarters. However, in cases where Korean laws or the headquarters' ESG policy conflict with local laws of the overseas subsidiaries, the local laws shall take precedence.

All laws mentioned in this policy are part of the legal framework of the Republic of Korea. However, if there are similar provisions in the local laws of the overseas subsidiaries, such local legal provisions shall take priority. In the event of any discrepancies in interpretation between the Korean and English versions, the Korean original shall be considered the official interpretation.

Certain departments specified in this policy may only exist at the headquarters. Nevertheless, in the case of overseas subsidiaries, departments that perform the same functions as those at the headquarters, departments delegated with authority from the headquarters, or the relevant headquarters departments responsible for such functions shall apply as the standard.

	ESG Management Policy	Num	YRC-24
		Modified date	2023.06.09
	Personal Data Protection Guidelines Policy	Page	1
		Department in charge	S&SHE Team

Table of Contents

Revision History

Version	Revision Date	Revision Details
0	12.10.12	Newly enacted
1	14.06.01	Change in the drafting entity due to team restructuring
2	15.09.21	Deletion of CCTV installation status information, revision of video surveillance operation and management policy
3	18.10.05	Revision of video surveillance operation and management policy
4	19.02.12	Reflection of amendments to the Personal Data Protection Act (enhanced breach reporting obligations, etc.)
5	23.06.08	Change in video information management officer and processing personnel

2023.06.09

Chapter 1 General Provisions

Article 1 (Purpose)

These Personal Data Protection Guidelines aim to establish detailed standards regarding the processing of personal data that YURA (hereinafter referred to as the "Company") must comply with under Article 12(1) of the Personal Data Protection Act (hereinafter referred to as the "Act"), including types of personal data breaches and preventive measures.

Article 2 (Definitions)

The definitions of terms used in these guidelines are as follows

1. "Personal Data Processing" refers to collecting, generating, recording, storing, retaining, processing, editing, retrieving, outputting, correcting, recovering, using, providing, disclosing, destroying, or any similar actions related to personal data.
2. "Data Subject" refers to the individual who can be identified by the processed information.
3. "Chief Information Security Officer " refers to the individual responsible for overseeing and making final decisions regarding the Company's information security and personal data protection.
4. "Personal Data Protection Officer " refers to the individual responsible for personal data processing within the Company, as specified in Article 32(2)(2) of the Enforcement Decree of the Personal Data Protection Act.
5. "Personal Data Protection Officer " refers to an employee designated by the Personal Data Protection Officer to perform practical tasks related to personal data protection.
6. "Personal Data Handler" refers to individuals processing personal data under the supervision of the Personal Data Protection Officer, including those directly responsible for personal data-related tasks and others who access personal data for business purposes.

7. "Personal Data Processing System" refers to a systematically organized database system that enables personal data processing.
8. "Access Log" refers to electronic records containing identifiers, access date/time, access location, performed tasks, and other details regarding access to the Personal Data Processing System by data subjects or personal data handlers.
9. "Video Surveillance System" refers to any device installed in a designated area to continuously capture images of individuals or objects and transmit them via wired or wireless networks, including Closed-Circuit Television (CCTV) and network cameras as defined in Article 3 of the Enforcement Decree.
10. "Personal Video Data" refers to video information captured and processed by video surveillance systems, which includes an individual's facial features, behavior, or other private aspects, allowing identification of that individual.
11. "Public Area" refers to locations such as parks, roads, subways, shopping malls, parking lots, and other places where data subjects have unrestricted access or passage.
12. "Processing" refers to actions related to video data, including input, storage, editing, deletion, playback, and other similar activities, excluding the collection of such data by CCTV.

Article 3 (Scope of Application)

These guidelines apply to all personnel of the Company and employees of external cooperating firms handling any form of personal data files, regardless of whether they are processed electronically or manually

Article 4 (Principles of Personal Data Protection)

① The purpose of collecting personal data must be clearly specified at the time of collection, and the Company shall process personal data only to the extent necessary to achieve that

specified purpose.

② Personal data must be accurate and kept up to date to reflect the factual status at the time of processing. During processing, appropriate measures shall be taken to prevent unauthorized alteration or damage to personal data due to intentional or negligent actions.

③ The Company shall ensure the safe management of personal data through appropriate technical, administrative, and physical security measures corresponding to the risk level and potential infringement on data subjects' rights.

④ Matters related to personal data processing, such as personal data processing policies, shall be publicly disclosed, and reasonable procedures shall be established to ensure data subjects' rights, including the right to request access.

⑤ Even when processing personal data within the necessary scope for achieving a specified purpose, methods that minimize the infringement of data subjects' privacy shall be selected whenever possible.

⑥ Even when the Company obtains the consent of data subjects for processing personal data under the Personal Data Protection Act, the processing shall be conducted in a manner that minimizes identification of specific individuals whenever feasible due to the nature of the tasks involved.

Article 5 (Operation and Management Policy for Video Surveillance Systems)

When establishing or amending the operation and management policy for video surveillance systems, the Company shall ensure that data subjects can easily access and review such policies.

Article 6 (Relationship with Other Guidelines)

Matters not specifically addressed in these guidelines shall be governed by the Standard Personal Information Protection Guidelines established by the Ministry of the Interior and Safety.

Chapter 2: Personal Data Protection Organization

Article 7 (Composition of the Personal Data Protection Organization)

① The Company shall establish a personal data protection organization responsible for handling personal data processing tasks efficiently and ensuring accountability.

Article 8 (Roles and Responsibilities)

① YURA shall designate an Information Security Officer responsible for overseeing information security and personal data processing.

② Pursuant to Paragraph 1, the Company shall appoint and operate the Head of the Support Division as the Chief Security Officer, who shall be responsible for overall information security.

③ The Information Security Officer shall perform the following duties:

1. Overall supervision of information security and personal data protection
2. Approval and announcement of the establishment and revision of information security and personal data protection guidelines
3. Review and approval of the current status of information security and personal data protection
4. Delivering messages regarding the commitment to information security and personal data protection to executives and employees

④ The Company shall establish an Information Security Committee composed of the Head of the Support Division, the Head of the HR & General Affairs Office, the Head of the HR Planning Team, the Head of the General Affairs Team, the Head of the Information Security Team, and the Head of the dedicated technical information security department (YURA IT Division)

⑤ The Information Security Committee shall perform the following duties:

1. Review of company-wide security strategies and implementation plans
2. Review of information security and personal data protection planning, budgeting, implementation, and audit results
3. Discussion of managerial, human, physical, and technical issues related to information security
4. Prior review and discussion of system operation policies when introducing information systems related to information security and personal data protection
5. Review of requirements for the establishment and revision of information security and personal data protection guidelines
6. Decision-making consultations in case of major security incidents or personal data breaches
7. Review of disciplinary actions for violations of personal data protection and security policies
8. Review of personnel security matters, such as security clearance for handling classified information
9. Review of disclosure and external provision of confidential documents and customer personal data

⑥ The Company shall appoint and operate the Head of the dedicated information security department as the Information Security Manager.

⑦ The Information Security Manager shall perform the following duties:

1. Overall operation and management of the personal data processing system
2. Management of measures to ensure the security of personal data
3. Supervision of the implementation of technical protection measures for personal data protection

4. General supervision of information security-related tasks and oversight
5. Development of detailed policies and activities for information security
6. Overall responsibility for security incident prevention and response activities
7. Improvement of regulations related to information security

⑧ The Information Security Manager shall designate and operate team members of the dedicated information security department as Information Security IT Officers and Personal Data IT Officers.

⑨ The Personal Data IT Officer shall support and perform the following tasks:

1. Management of access rights and passwords for the personal data processing system
2. Installation and operation of access control systems
3. Encryption of personal data
4. Retention and protection against forgery or falsification of access records
5. Installation and operation of security programs
6. Monitoring of the personal data processing system
7. Network security inspections
8. Annual compliance audits of information security guidelines in business departments
9. Conducting personal data impact assessments, if necessary

⑩ The Information Security IT Officer shall support and perform the following tasks

1. Assistance with the duties of the Information Security Manager
2. Establishment of measures to ensure the security of personal data protection
3. Planning, implementation, and review of the annual information security activity plan
4. Planning of budget, schedules, procedures, and operational measures related to information security activities
5. Technical feasibility assessment of security measures implementation
6. Discussion of IT operation policies related to security
7. Incident response for security issues, including reporting and handling security incidents

8. Conducting security guidance and training for information systems
9. Management of information assets
10. Management of access rights and accounts for information systems
11. Regular inspection and training on information system infrastructure
12. Vulnerability assessment of information systems and reporting of results

⑪ The Company shall designate and operate the Head of the HR Planning Team (CPO) as the Personal Data Protection Officer instead of establishing a separate Personal Data Protection Team.

⑫ The Personal Data Protection Officer shall perform the following duties:

1. Establishment, implementation, and management of personal data protection policies, guidelines, and related regulations
2. Handling and processing of requests from data subjects, such as access requests and complaints related to personal data breaches
3. Supervision and inspection of personal data processing practices
4. Compilation and management of personal data protection-related statistics and records
5. Monitoring compliance with personal data protection requirements
6. Conducting personal data protection education and other necessary activities for personal data protection
7. Operation of Personal Data Protection Day, if necessary

⑬ The Personal Data Protection Officer shall designate and operate HR Planning Team members as Personal Data Protection Officers.

⑭ The Personal Data Protection Officer shall perform the following duties:

1. Establishment of personal data protection guidelines and personal data processing policies
2. Development of internal management plans

3. Regular audits of compliance with the personal data protection management system
4. Planning and implementation of personal data protection education
5. Record and management of personal data files and personal data file destruction logs
6. Responding to data subjects' requests for access, correction, deletion, and suspension of processing of personal data
7. Collection of personal data protection pledges
8. Response to personal data breaches

Article 9 (Disclosure of the Personal Data Protection Officer)

① In the event of the designation or change of the Personal Data Protection Officer, the designation or change, along with the name, department, and contact information (such as telephone number), shall be disclosed.

② When disclosing the Personal Data Protection Officer, the contact information for handling complaints and inquiries related to personal data protection shall also be disclosed. However, the names, department names, and contact details of the Information Security Officer and other responsible personnel handling personal data protection may be included together.

Article 10 (Establishment and Operation of the Internal Personal Data Management Plan)

① The Personal Data Protection Officer shall collect opinions from the heads of personal data-handling departments and establish an annual internal personal data management plan.

② The internal personal data management plan shall include comprehensive measures for personal data protection, such as technical and administrative security controls at each stage of personal data processing, a personal data protection education plan, periodic internal audits, and procedures for responding to and remedying personal data breaches.

Chapter 3: Standards for Personal Data Processing

Section 1: Processing of Personal Data Collection and Use

Article 11 (Collection of Personal Data)

① "Collection" of personal data refers not only to directly obtaining personal data such as name, address, and phone number from the Data Subject but also to acquiring any form of personal data related to the Data Subject.

② YURA may collect personal data only under the following circumstances and may use it within the scope of the specified purpose

1. When prior consent has been obtained from the Data Subject.
2. When specific laws explicitly stipulate or permit the collection and use of personal data.
3. When fulfilling legally mandated obligations is impossible or significantly difficult without collecting and using personal data.
4. When it is impossible or significantly difficult to perform duties prescribed by law without collecting and using personal data.
5. When executing a contract with the Data Subject and fulfilling contractual obligations is impossible or significantly difficult without collecting and using personal data.
6. When a pressing situation necessitates the collection and use of personal data to prevent harm to the life, body, or property of the Data Subject or a third party (any entity other than the Data Subject), but the Data Subject or their legal representative is unable to express intent or cannot be reached due to an unknown address.
7. When it is necessary to achieve legitimate interests as stipulated by law or a contract with

the Data Subject, and such necessity clearly outweighs the Data Subject's right to decide whether and to what extent their personal data is collected and used. However, in such cases, the collection and use of personal data must be substantially related to YURA's legitimate interests and must not exceed a reasonable scope.

③ When obtaining consent under Item 1 of Paragraph 2, the following details must be provided to the Data Subject, and any changes to these details must also be communicated and consent must be obtained again

1. Purpose of collecting and using personal data
2. Items of personal data to be collected
3. Retention and usage period of personal data
4. The fact that the Data Subject has the right to refuse consent and the consequences of refusal, if applicable

④ When collecting personal data directly from the Data Subject through a business card or a similar medium (hereinafter referred to as "business card, etc."), the collected data may only be used within a socially acceptable scope where the Data Subject's consent can be reasonably inferred based on the circumstances in which the business card, etc., was provided.

⑤ When the Data Subject, as a counterparty in a contract, conducts legal acts or makes declarations of intent through an agent, personal data of the agent may be collected solely for the purpose of verifying the agent's authority.

⑥ In cases where an employer and an employee enter into an employment contract, personal data may be collected and used without the employee's consent for purposes such as wage payment, training, certificate issuance, and employee welfare provision in accordance with Article 2, Item 5 of the Labor Standards Act.

Article 12 (Cases Where Prior Consent of the Data Subject Cannot Be Obtained)

If the Data Subject or their legal representative is unable to express intent or cannot be reached due to an unknown address, and it is deemed necessary to collect, use, or provide personal data to protect the urgent life, body, or property interests of the Data Subject or a third party, YURA may proceed without prior consent. However, once the reason for this necessity is resolved, the processing of personal data must be immediately discontinued, and the Data Subject must be informed of the collection or use of their personal data without prior consent, including the reason and details of its use.

Article 13 (Notification of Personal Data Collection Source, etc.)

When YURA processes personal data collected from a source other than the Data Subject, it must inform the Data Subject of the source of collection, the purpose of processing, and the fact that the Data Subject has the right to request the suspension of personal data processing within three (3) days from the date of request, unless there is a legitimate reason not to do so.

Section 2: Retention and Management of Personal Data

Article 14 (Retention of Personal Data in Accordance with Laws and Regulations)

If the destruction of personal data is prohibited by other laws, the relevant personal data or personal data file must be explicitly marked as retained

Section 3: Processing of Personal Data Provision

Article 15 (Provision of Personal Data)

① Personal data may be provided to a third party (including sharing) in any of the following cases:

1. When consent has been obtained from the Data Subject.
2. When special provisions exist in other laws or when it is unavoidable to comply with legal obligations.
3. When the Data Subject or their legal representative is unable to express intent or cannot be reached due to an unknown address, and it is deemed necessary to protect the urgent life, body, or property interests of the Data Subject or a third party.
4. When personal data is provided in a manner that prevents the identification of a specific individual for statistical or academic research purposes.

② When obtaining consent under Item 1 of Paragraph 1, the following details must be provided to the Data Subject, and any changes must be communicated and consent must be obtained again:

1. Recipient of the personal data
2. Purpose of personal data use by the recipient
3. Items of personal data to be provided
4. Retention and usage period of personal data by the recipient
5. The fact that the Data Subject has the right to refuse consent and the consequences of refusal, if applicable
6. If the Data Subject is informed of the recipient of their personal data, the recipient's name (or organization name, if a corporation or entity) and contact information must be provided.

Article 16 (Use of Personal Data for Purposes Other Than Originally Intended, etc.)

① YURA shall not use personal data beyond the scope stipulated in Article 10, Paragraph 1, nor

shall it provide personal data to third parties beyond the scope stipulated in Article 14, Paragraph 1.

② Notwithstanding Paragraph 1, YURA may use personal data for purposes other than originally intended or provide it to third parties under any of the following circumstances, except when doing so may unduly infringe upon the interests of the Data Subject or a third party

1. When consent has been obtained from the Data Subject.
2. When specific provisions in other laws exist.
3. When the Data Subject or their legal representative is unable to express intent or cannot be reached due to an unknown address, and it is deemed necessary to protect the urgent life, body, or property interests of the Data Subject or a third party.
4. When personal data is provided in a manner that prevents the identification of a specific individual for statistical or academic research purposes.

③ When providing personal data to a third party for purposes other than originally intended under Paragraph 2, YURA shall, at the time of provision or after the fact if necessary, impose restrictions on the recipient regarding the purpose, method, duration, and form of use of the personal data and request in writing (including electronic documents) that necessary security measures be taken. If necessary, YURA may also make additional requests after the data has been provided. In such cases, the recipient must comply with these requests and notify YURA in writing of the actions taken.

④ When providing personal data to a third party for purposes other than originally intended under Paragraph 2, YURA and the recipient must clearly define their respective responsibilities for the security of personal data.

⑤ When obtaining separate consent under Item 1 of Paragraph 2, the following details must be provided to the Data Subject, and any changes must be communicated and consent must be obtained again

1. Recipient of the personal data
2. Purpose of personal data use by the recipient
3. Items of personal data to be provided
4. Retention and usage period of personal data by the recipient
5. The fact that the Data Subject has the right to refuse consent and the consequences of refusal, if applicable
6. When informing the Data Subject about the recipient of their personal data under Item 1 of Paragraph 2, the recipient's name (or organization name, if a corporation or entity) and contact information must be provided.
7. When providing personal data to a third party under Item 4 of Paragraph 2, the data must be provided in a form that prevents the identification of specific individuals even when combined with other information.

⑥ When informing the Data Subject about the recipient of their personal data under Item 1 of Paragraph 2, the recipient's name (or organization name, if a corporation or entity) and contact information must be provided.

⑦ When providing personal data to a third party under Item 4 of Paragraph 2, the data must be provided in a form that prevents the identification of specific individuals even when combined with other information.

Section 4: Disposal of Personal Data

Article 17 (Methods and Procedures for Disposal of Personal Data)

① If the retention period of personal data has expired, the data shall be destroyed within five (5) days from the expiration date, unless there is a legitimate reason to retain it. If personal

data has become unnecessary due to the achievement of its processing purpose, discontinuation of the relevant service, or business closure, the data shall be destroyed within five (5) days from the date it is deemed unnecessary, unless a legitimate reason exists to retain it.

② Records of personal data disposal must be maintained, and the disposal process must be executed and verified under the responsibility of the Personal Data Protection Officer.

③ The Personal Data Protection Officer must verify and confirm the results of the data disposal process.

④ Personal data subject to disposal includes not only the personal data provided by the Data Subject but also data generated during service provision (such as login records, IP addresses, cookies, payment records) and backup files containing personal data.

⑤ When disposing of personal data, it must be irreversibly destroyed in a manner that prevents identification, recovery, or reproduction.

1. Printed personal data: Must be shredded or incinerated.
2. Electronically stored personal data: Must be destroyed using technical methods that make it irrecoverable.

⑥ If personal data cannot be disposed of due to legal obligations, the relevant personal data or personal data file must be stored and managed separately from other personal data.

Section 5: Delegation of Personal Data Processing

Article 18 (Considerations for Selecting Entrusted Parties)

① When entrusting personal data processing tasks, YURA must comprehensively consider factors such as personnel, physical infrastructure, financial capability, technical expertise, and liability when selecting the entrusted party (processor).

② When entrusting personal data processing tasks, YURA must assess and take necessary measures to prevent potential issues, such as delays in processing, unnecessary requests for personal data, or unfair processing practices by the entrusted party.

Article 19 (Obligations of the Entrusted Party to Protect Personal Data)

The entrusted party (processor) must implement administrative, technical, and physical security measures in accordance with the "Personal Data Security Measures Standards" to protect the entrusted personal data.

Article 20 (Relationship Between the Data Subject and Sub-Entrusted Parties)

① The Data Subject may claim compensation for damages caused by a sub-entrusted party (sub-processor) that has been entrusted with the processing of personal data.

③ The sub-entrustment of personal data processing shall comply with Article 26 of the Personal Data Protection Act.

Section 6: Consent for Personal Data Processing

Article 21 (Methods of Obtaining Consent)

① When obtaining consent from the Data Subject for the collection and use of personal data, YURA must distinguish between the minimum necessary personal data for providing basic goods or services and additional personal data required for supplementary goods or services and inform the Data Subject accordingly.

② If consent is required for personal data processing, YURA must clarify cases where consent is necessary and cases where it is not, notifying the Data Subject when consent is not

required and explaining the reasons.

③ When obtaining separate consent, YURA must ensure that the Data Subject can indicate their consent separately from other processing purposes.

④ If consent is obtained via telephone, the Data Subject must be informed that the call is being recorded.

⑤ The following methods may be used to obtain the Data Subject's consent:

1. Providing a written consent form directly to the Data Subject or sending it via mail or fax, and obtaining a signed or stamped consent form.
2. Informing the Data Subject of the consent details over the phone and verifying their intent.
3. Informing the Data Subject of the consent details over the phone, allowing them to review the consent terms via an internet link, and then confirming their intent over the phone.
4. Posting the consent details on a website and allowing the Data Subject to indicate consent.
5. Sending the consent details via email and receiving an email response indicating consent.
6. Any other method equivalent to the above that allows the Data Subject to be informed of the consent details and verify their intent.

⑥ For obtaining consent from a legal representative of a child under the age of 14, personal data such as the legal representative's name and contact information may be collected directly from the child.

⑦ When processing personal data of a child under 14, consent must be obtained from their legal representative in accordance with these guidelines. In this case, only the minimum necessary information to obtain the legal representative's consent may be collected from the child without separate consent.

Article 22 (Consent of the Legal Representative)

① When collecting the name and contact information of a legal representative, YURA must

inform the child of the Company's identity, contact details, and the reason for collecting the legal representative's name and contact information.

② The methods specified in Article 13, Paragraph 5 for obtaining consent shall also apply when obtaining consent from a legal representative.

③ The personal data of the legal representative collected under this Article shall be used solely for obtaining consent. If the legal representative refuses consent or does not confirm their consent within five (5) days from the date of collection, the collected data shall be destroyed.

Article 23 (Consent for Processing of Sensitive Information)

① When obtaining consent from the Data Subject for the processing of sensitive information, YURA must ensure that sensitive information is distinguished from other personal data and that the Data Subject can provide separate consent specifically for sensitive information.

② When obtaining consent under Paragraph 1, the following details must be provided to the Data Subject, and any changes must be communicated and consent must be obtained again

1. Purpose of collecting and using sensitive information
2. Items of sensitive information to be collected
3. Retention and usage period of sensitive information
4. The fact that the Data Subject has the right to refuse consent and the consequences of refusal, if applicable

Article 24 (Consent for Processing of Unique Identifiers)

① When obtaining consent from the Data Subject for the processing of unique identifiers, YURA must ensure that unique identifiers are distinguished from other personal data and that the Data Subject can provide separate consent specifically for unique identifiers.

② When obtaining consent under Paragraph 1, the following details must be provided to the

Data Subject, and any changes must be communicated and consent must be obtained again

1. Purpose of collecting and using unique identifiers
2. Items of unique identifiers to be collected
3. Retention and usage period of unique identifiers
4. The fact that the Data Subject has the right to refuse consent and the consequences of refusal, if applicable

Section 7: Miscellaneous Personal Data Processing

Article 25 (Implementation of Personal Data Impact Assessments)

① If YURA develops a new service that may pose a risk of personal data infringement due to the operation of the associated personal data file, a Personal Data Impact Assessment (PIA) shall be conducted to analyze risk factors and derive improvement measures.

② The department responsible for developing a new service shall prepare a pre-assessment inquiry for the Personal Data Impact Assessment and, if at least one of the criteria applies, submit a request for the assessment to the YURA IT Division Information Operations Team.

③ The YURA IT Division IT Information Operations Team shall conduct the Personal Data Impact Assessment in accordance with the "Guidelines for Conducting Personal Data Impact Assessments" issued by the Ministry of the Interior and Safety and report the results to the Information Security Committee.

④ The Information Security Committee shall review the results of the Personal Data Impact Assessment Report and ensure that the new service development department incorporates the findings into its service planning

Article 26 (Provision of Membership Registration Methods Other than Personal Identification

Number)

If the number of data subjects using YURA's website exceeds an average of 10,000 per day for three consecutive months at the end of the previous year, YURA must explicitly notify users, through the membership registration screen, that they may register as members using an alternative method instead of a Personal Identification Number (PIN).

In this case, both the membership registration method using a Personal Identification Number (PIN) and the alternative registration method must be provided on a single screen.

Article 27 (Supervision of Personal Data Handlers)

① The number of Personal Data Handlers shall be minimized to the extent necessary for business operations, and their scope of personal data processing shall be strictly limited to what is essential for performing their duties.

② Access rights to the Personal Data Processing System shall be assigned in a differentiated manner based on job functions, ensuring that each employee has access only to the data necessary for their specific tasks. Measures must also be implemented to manage and regularly review access rights.

③ YURA shall ensure appropriate supervision and management of Personal Data Handlers, such as requiring them to sign a Personal Data Protection Pledge. In the event of personnel transfers or role changes, the Personal Data Handler's access rights must be modified or revoked as necessary.

Article 28 (Personal Data Protection Pledge)

① The Personal Data Protection Officer shall obtain written Personal Data Protection Pledges from all Personal Data Handlers and submit them to the Chief Executive Officer.

② If a new Personal Data Handler is designated, they must sign a Personal Data Protection Pledge and submit it to the Personal Data Protection Team before assuming their

responsibilities.

Chapter 4: Guarantee of Data Subject Rights

Article 29 (Request for Access to Personal Data)

The personal data files retained by YURA may be subject to access requests in accordance with Article 35 (Access to Personal Data) of the Personal Data Protection Act. Access to personal data may be restricted pursuant to Paragraph 4 of Article 35 of the Act in the following cases:

1. When access is prohibited or restricted by law.
2. When there is a concern that access may cause harm to another person's life or physical safety or unfairly infringe on another person's property or other interests.

Article 30 (Request for Correction or Deletion of Personal Data)

If a request for the correction or deletion of personal data files retained by YURA is made in accordance with Article 36 of the Personal Data Protection Act, the Company shall investigate the relevant personal data and take necessary measures, such as correction or deletion, within ten (10) days from the date of the request, unless there is a legitimate reason to refuse. The results of such measures shall be notified to the data subject. However, if the collection of such personal data is explicitly specified by other laws or regulations, the data subject may not request its deletion.

Article 31 (Request for Suspension of Personal Data Processing)

① The personal data files retained by YURA may be subject to a request for suspension of processing in accordance with Article 37 of the Personal Data Protection Act. However, such a request may be denied pursuant to Paragraph 2 of Article 37 of the Act in the following cases:

1. When access is prohibited or restricted by law.
2. When there is a concern that suspension of processing may cause harm to another person's life or physical safety or unfairly infringe on another person's property or other interests.
3. When non-processing of personal data makes it difficult to fulfill a contractual obligation agreed upon with the data subject, and the data subject has not explicitly expressed their intention to terminate the contract.

Article 32 (Method of Requesting Access, Correction/Deletion, and Suspension of Processing of Personal Data)

The contact information of the Personal Data Protection Officer and related forms shall be posted on the Company's website to ensure that data subjects can access and utilize them.

Chapter 5: Establishment of Personal Data Processing Policy

Article 33 (Disclosure of the Personal Data Processing Policy)

① When establishing or revising the Personal Data Processing Policy, it must be continuously published on the official website (www.yuracorp.co.kr). In this case, the title "Personal Data Processing Policy" must be used, and font size, color, and other design elements must be utilized to distinguish it from other notices, ensuring that data subjects can easily recognize it.

② If the Company does not operate a website or if there are technical issues with website management, the Personal Data Processing Policy must be disclosed using one or more methods specified in Article 31, Paragraph 3 of the Enforcement Decree. Even in such cases, the title "Personal Data Processing Policy" must be used, and design elements such as font size and color must be applied to distinguish it from other notices, ensuring that data subjects can easily recognize it.

③ If the Personal Data Processing Policy is disclosed through the method specified in Paragraph 2, it must be continuously included in each publication of the Company's brochures, newsletters, promotional materials, or billing statements.

Article 34 (Changes to the Personal Data Processing Policy)

When the Personal Data Processing Policy is revised, the timing of the changes and the details of the amendments must be continuously disclosed. The revised content must be presented in a way that allows data subjects to easily recognize the differences by comparing the previous and new versions.

Article 35 (Standards for Drafting the Personal Data Processing Policy)

① When drafting the Personal Data Processing Policy, the required information specified in Article 35 must be explicitly categorized and expressed in clear and precise language.

② The policy must clarify that the personal data being processed is limited to the minimum necessary for the intended purpose.

③ If additional personal data is processed beyond the minimum necessary for the intended purpose, such as for personalized services, these categories must be distinctly identified.

Article 36 (Mandatory Information to be Included)

When drafting the Personal Data Processing Policy, it must include all of the following:

1. Purpose of personal data processing
2. Period of personal data processing and retention
3. Provision of personal data to third parties (if applicable)
4. Delegation of personal data processing (if applicable)
5. Rights and obligations of data subjects and the methods for exercising them
6. Categories of personal data being processed
7. Procedures for the destruction of personal data
8. Information regarding the Personal Data Protection Officer
9. Information regarding changes to the Personal Data Processing Policy
10. Measures to ensure the security of personal data

Article 37 (Optional Information to be Included)

In addition to the mandatory information specified in Article 36, the Personal Data Processing Policy may also include the following:

1. Remedies available for data subjects in case of infringement of their rights
2. The department responsible for receiving and handling requests for access to personal data

Chapter 6: Notification of Personal Data Breach

Article 38 (Personal Data Breach)

A personal data breach refers to the loss of control by the Personal Data Protection Officer over a data subject's personal data, or unauthorized access to such data without legal grounds or the

voluntary decision of the Personal Data Protection Officer. A breach is deemed to have occurred in any of the following cases:

1. Loss or theft of documents containing personal data, portable storage devices, or portable computers.
2. Unauthorized access to databases or other personal data processing systems by individuals without legitimate access rights.
3. Accidental disclosure of files, paper documents, or other storage media containing personal data to unauthorized individuals due to the intent or negligence of a personal data processor.
4. Any other situation in which personal data is disclosed to unauthorized individuals or access to personal data processing systems is inadvertently enabled.

Article 39 (Timing and Content of Notification)

① Once a personal data breach has been confirmed, data subjects must be notified within five (5) days, unless there is a justifiable reason for delay. The notification must include the following details:

1. Categories of personal data that were breached.
2. Time of occurrence and the circumstances of the breach.
3. Measures that data subjects can take to minimize potential damage.
4. The response actions taken by the personal data processor and procedures for seeking remedies.
5. Contact details of the department responsible for handling reports in case data subjects suffer damages.

② If there is a time gap between the actual occurrence of the data breach and the time it was discovered (as per Paragraph 1, Clause 2), the entity responsible must provide evidence of

whether negligence was involved.

③ After taking the measures specified in Paragraph 1, the following information must be initially notified to data subjects, with further details provided as soon as they become available:

1. Confirmation that a personal data breach has occurred.
2. Any details confirmed from the notification items specified in Article 27, Paragraph 1.

Article 40 (Notification Method)

① When notifying data subjects about the details specified in Article 27, Paragraph 1, the notification must be made without delay using written documents, email, fax, telephone, mobile text messages, or similar means.

② In addition to the notification methods in Paragraph 1, the details specified in Article 27, Paragraph 1 may also be published on the Company's website.

Article 41 (Reporting of Personal Data Breach)

① In the event that the personal information of more than 1,000 data subjects is leaked, the Company must notify the data subjects and report the notification and the measures taken to the designated data protection authority or the relevant agency designated by the authority in the country where the overseas subsidaries are located within five days.

② The report must be submitted using Annex Form No. 1: Personal Data Breach Report.

③ If there is insufficient time to report the breach via email, fax, or an online platform, or in cases of exceptional circumstances, the breach may first be reported via telephone in accordance with Article 27, Paragraph 1, followed by the formal submission of Annex Form No. 1: Personal Data Breach Report.

④ If a personal data breach affecting 1,000 or more data subjects occurs, in addition to the notification in Article 37, Paragraph 1, the details specified in Article 37, Paragraph 1 must be

posted on the Company's website for at least seven (7) days in a manner that data subjects can easily recognize.

Chapter 7: Installation and Operation of Video Surveillance Equipment

Section 1: Installation of Video Surveillance Equipment

Article 42 (Scope of Application)

This policy applies to video surveillance equipment installed and operated by YURA in public areas, as well as personal video information processed through such equipment.

Article 43 (Legal Basis and Purpose of Video Surveillance Equipment Installation)

The video surveillance equipment operated by YURA is installed in accordance with Article 6, Paragraph 1, Item 11 of the Parking Lot Act Enforcement Rules and Article 25, Paragraph 3 of the Personal Data Protection Act. The purpose of this installation includes ensuring user safety, crime prevention, securing evidence, facility management, and fire prevention.

Article 44 (Current Status of Video Surveillance Equipment Installation)

The current status of YURA's video surveillance equipment installation is detailed in Appendix 1.

Article 45 (Designation of Responsible Personnel and Departments)

① YURA designates the GA Team Leader as the Personal Video Data Management Officer, who is responsible for overseeing and managing tasks related to the processing of personal video data, as well as the Personal Video Data Operations Manager.

② The Personal Video Data Protection Officer, as designated under Paragraph 1, shall perform

the following duties in accordance with Article 31, Paragraph 2 of the Personal Data Protection Act

1. Establishment and implementation of personal video information protection plans.
2. Regular assessment and improvement of personal video information processing practices.
3. Handling complaints and providing remedies related to personal video information processing.
4. Establishment of internal control systems to prevent leakage, misuse, or abuse of personal video information.
5. Development and implementation of personal video information protection training programs.
6. Supervision of the protection and destruction of personal video information files.
7. Any other necessary measures for the protection of personal video information.

Article 46 (Installation of Signage)

① The Personal Video Data Protection Officer shall install signage indicating the operation of video surveillance equipment in compliance with Article 25, Paragraph 4 of the Personal Data Protection Act. The signage shall include the following details:

1. Purpose and location of installation
2. Scope and duration of recording
3. Name or title and contact information of the responsible officer
4. If the operation of the video surveillance equipment is outsourced, the name and contact information of the contractor

② The signage must be installed in easily visible locations within the recording area, allowing individuals to recognize it effortlessly. YURA shall determine the size and placement of the signage

at its discretion within this framework.

Section 2: Processing of Personal Video Data

Article 47 (Recording Time, Retention Period, Storage Location, Equipment Specifications, and Processing Methods)

① YURA continuously records video surveillance footage 24 hours a day, in accordance with the legal basis and purpose of installation.

② The retention period for personal video data is set to a minimum of 30 days and is stored on the hard disk of the video data processing system located in the designated area specified by the GA Team. Upon expiration of the designated retention period, the data must be promptly deleted, unless otherwise stipulated by applicable laws and regulations that require a different retention period.

③ The video surveillance equipment specifications include a resolution of 410,000 pixels, minimum illumination of 0.002 Lux, and a horizontal resolution of at least 560 lines. The equipment does not include arbitrary manipulation or audio recording functions.

④ Methods of destroying personal video information include:

1. Shredding or incineration of printed materials (such as photographs) containing personal video information.
2. Automatic deletion of electronically stored personal video information on the digital video recording (DVR) system after 30 days.

Article 48 (Methods and Locations for Viewing Video Information by Operators)

① Access to personal video information transmitted by video surveillance equipment is restricted to authorized personnel. Viewing or playback is only permitted upon approval from the Personal Video Data Protection Officer.

- Personal Video Data Protection Officer
- Personal Video Data Management Officer
- Individuals approved by the Personal Video Data Protection Officer

② The location for accessing personal video data is designated by the GA Team and classified as a restricted access area.

Article 49 (Restrictions on Use and Provision of Personal Video Data to Third Parties)

① YURA does not use personal video information for purposes other than its original intent or provide it to third parties, except in the following cases

1. When consent is obtained from the data subject.
2. When required by special provisions of other laws.
3. When the data subject or their legal representative is unable to express consent due to incapacity, or when prior consent cannot be obtained due to an unknown address, and provision is deemed necessary to protect the urgent life, body, or property interests of the data subject or a third party.
4. When required for statistical or academic research purposes, provided that the data is processed in a way that prevents identification of individuals.

Article 50 (Records and Management of Use, Third-Party Provision, and Disposal)

① YURA shall record and manage the following items when using personal video information for purposes other than collection or providing it to a third party

1. Name of the personal video information file
2. Name of the entity utilizing or receiving the information
3. Purpose of use or provision
4. Legal basis for use or provision, if applicable

5. Period of use or provision, if specified
6. Form of use or provision

② When disposing of personal video information, the following items shall be recorded and managed

1. Name of the personal video information file being disposed of
2. Date and time of disposal (if automatically deleted according to a predetermined schedule, the deletion cycle and confirmation time of automatic deletion)
3. Person responsible for the disposal of personal video information

Article 51 (Delegation of Installation and Management of Video Information Processing Devices)

① If YURA entrusts a third party with the installation and operation of video information processing devices in accordance with Article 26, Paragraph 1 of the Enforcement Decree, it shall disclose the trustee's name through the signage specified in Article 24 of the Enforcement Decree and the operational and management policy of video information processing devices specified in Article 27 of the Enforcement Decree, ensuring that the data subjects can verify the information at any time.

② If YURA entrusts a third party with the installation and operation of video information processing devices, it shall supervise and manage whether the entrusted party processes personal video information securely.

Section 3: Requests for Access to Personal Video Information

Article 52 (Measures for Requests to Access Personal Video Information by Data Subjects)

① A data subject may request access to or confirmation of the existence of personal video information by submitting a request form to YURA's Personal Data Protection Officer. In this case, the personal video information that may be requested for access shall be limited to video footage in which the data subject appears and personal video information necessary to protect the urgent life, body, or property interests of the data subject.

② YURA shall take necessary measures without delay upon receiving a request for access or confirmation of personal video information. In doing so, YURA shall verify the data subject's identity or legal representation by requesting an identification document such as a resident registration card, driver's license, or passport.

③ YURA may deny a request for access or confirmation of personal video information in the following cases and shall notify the data subject in writing within ten days, specifying the reason for denial

1. If the retention period of personal video information has expired and it has been disposed of
2. If there are other legitimate reasons for refusing the request

④ The Personal Data Protection Officer shall record and manage the following details when taking actions under Paragraphs 2 and 3:

1. Name and contact information of the data subject requesting access
2. Name and content of the requested personal video information file
3. Purpose of the request
4. Specific reason for denial, if applicable
5. If a copy of the personal video information was provided, the content and reason for provision

⑤ If a data subject requests YURA to dispose of their personal video information, the disposal request shall only apply to the personal video information previously requested for retention under Paragraph 1. YURA shall record and manage details of any such disposal action taken.

Article 53 (Personal Video Information Management Log)

YURA shall record and manage the following items using the 'Personal Video Information Management Log'

1. When personal video information is used for purposes other than collection or provided to a third party
2. When personal video information is disposed of
3. When a data subject requests access to or confirmation of the existence of personal video information, and corresponding measures are taken

Article 54 (Protection of Personal Video Information of Non-Data Subjects)

When taking measures under Article 14, Paragraph 2, YURA shall implement protective measures to ensure that the identity of non-data subjects is not recognizable or to prevent any infringement of their privacy if their personal video information is clearly identifiable.

Section 4: Protection Measures for Personal Video Information

Article 55 (Measures to Ensure the Security of Personal Video Information)

YURA shall take the following measures to prevent the loss, theft, leakage, alteration, or damage of personal video information, in accordance with Article 29 of the Personal Data Protection Act (PDPA) and Article 30, Paragraph 1 of the Enforcement Decree

1. Establishment and implementation of an internal management plan for the secure handling of personal video information
2. Access control and restriction of access rights to personal video information
3. Application of technologies for secure storage and transmission of personal video information (e.g., encryption for secure transmission in network cameras, password protection for personal video information files)
4. Storage and protection against forgery or alteration of processing records (e.g., recording and managing the date and time of creation, purpose of access, identity of the person accessing, and date and time of access)
5. Physical security measures such as secure storage facilities or installation of locking mechanisms

Article 56 (Inspection of Installation and Operation of Personal Video Information Processing Devices)

① YURA shall make active efforts, including conducting internal inspections, to prevent any potential infringement of personal video information due to the installation and operation of video information processing devices.

Supplementary Provisions

This Personal Data Protection Policy shall take effect from November 19, 2012. In case of any additions, deletions, or modifications due to changes in laws or policies, all employees shall be notified at least seven days prior to the effective date of such changes through the Company announcements.