Security Level	Confidential	Document No.	CKR-HR-013
Document Owner	Department Head	Department	HR, IT & Admin

	Human Resources		
	Personal Information Protection Management Regulations	Amendment Date	
		Structure	6 Chapters / 33 Articles

CMIC Korea Co., Ltd.

Chapter 1 General Provisions

Article 1 (Purpose)

The purpose of these Regulations (hereinafter referred to as the “Regulations”) is, in accordance with the “Personal Information Protection Act” (including all subsequent amendments), to set forth detailed matters concerning the criteria for the collection, use, provision and processing of personal information of CMIC Korea Co., Ltd. (hereinafter referred to as the “Company”), as well as the types of personal-information infringement and preventive measures, the internal management plan, and other related matters, thereby promoting stable management of personal-information protection.

Article 2 (Scope of Application)

These Regulations apply to all personal-information protection-related affairs in which the Company operates personal-information files in any form, including electronic files, printed documents, and paper records, and shall govern except as otherwise specifically provided by other statutes or regulations.

Article 3 (Definitions)

The definitions of the terms used in these Regulations are as follows:

1. “Personal information” means information relating to an individual, including the name, resident registration number and images, etc., by which the individual can be identified (including information by which the individual can be readily identified in combination with other information, even if the information alone is insufficient to identify a specific individual).
2. “Processing of personal information” means the collection, generation, recording, storage, retention, working, editing, search, output, correction, restoration, use, provision, disclosure, destruction, and any other act similar thereto with respect to personal information.
3. “Data subject” means an individual who is identifiable through the information being processed and who is the subject of such information.
4. “Personal information file” means a set of personal information arranged or organized systematically according to certain rules so that personal information can be easily retrieved.
5. “Personal information controller” means a public institution, juristic person, organization or individual that processes personal information directly or through another person to operate personal-information files for the purpose of its business.
6. “Privacy Officer” means the person who takes overall responsibility for the affairs relating to the processing of personal information, who falls under Article 31 of the Personal Information Protection Act.
7. “Personal Information Protection Manager by Field” means a person (the head of a department) who assists the Privacy Officer and oversees and manages practical affairs concerning personal-information protection.
8. “Person handling personal information” means a person who processes personal information under the direction and supervision of the personal information controller so that personal information can be safely managed when processing personal information (including officers and employees, dispatched workers, part-time workers, etc.).
9. “Personal-information processing system” means a database system organized systematically so as to be capable of processing personal information.
10. “Unique identification information” means identification information given for the purpose of uniquely distinguishing an individual under statute, and refers to the resident registration number under the Resident Registration Act, the passport number under the Passport Act, the driver’s license number under the Road Traffic Act, and the alien registration number under the Immigration Act.

11. “Biometric information” means information on the physical, physiological or behavioral characteristics by which an individual can be identified, such as fingerprints, face, iris, vein, voice, and handwriting (signature), as well as information processed or generated therefrom.
12. “Sensitive information” means information concerning ideology, beliefs, joining/withdrawal from a trade union or political party, political opinion, health information, sex life, etc.; genetic information obtained from genetic testing, etc.; information falling under criminal record data under Article 2(5) of the Act on the Lapse of Criminal Sentences; and other personal information that is likely to substantially infringe upon the privacy of the data subject.
13. “Auxiliary storage media” means storage media on which data can be stored, such as external hard disk drives (HDD), USB memory sticks, CDs (Compact Disks), and DVDs (Digital Versatile Disks), which can be easily separated from a personal-information processing system or personal computer (PC).
14. “Access record” means an electronic record that enables the identification of the fact that a person handling personal information, etc., has accessed a personal-information processing system, including the account, time of access, accessor’s information, and details of the work performed.
15. “Collection of personal information” means not only directly receiving information such as the name, address, and telephone number from the data subject, but also acquiring all forms of personal information about the data subject.
16. “Leakage of personal information” means a state where, not in accordance with statutes or with the free will and lawful procedures of the personal information controller, personal information of the data subject has gone beyond the management/control of the personal information controller and has been made accessible to a person without authority, and includes any of the following cases:
    a. Where a document, mobile storage device, portable computer, etc., containing personal information has been lost or stolen;
    b. Where a person without normal authority has gained access to a personal-information processing system, such as a database in which personal information is stored;
    c. Where, due to intent or negligence of the personal information controller, a file or paper document, or other storage medium containing personal information has been mistakenly delivered to a person without authority;
    d. Other cases where personal information has been delivered to a person without authority or access to a personal-information processing system, etc., has been made possible.
17. “Third party” means a person other than the personal information controller who has the right of control or management over personal information.
18. “Provision to a third party” means any act by which the personal information controller transfers the right of control/management over personal information to a third party other than itself, such as physical transfer of a storage medium of personal information, printouts or booklets containing personal information; transmission of personal information via networks; granting access privileges over personal information to a third party; and information-sharing between the personal information controller and a third party, so that the third party can process personal information.
19. “Video information processing device” means a device permanently installed in a certain location to film images of persons or objects or to transmit them via wired/wireless networks, and refers to the following devices:
    e. Closed-circuit television: a device that records images, etc., through a camera permanently installed in a certain location, or transmits such images via a wired/wireless closed-circuit transmission line, and a device that records and retains the images so filmed or transmitted;
    f. Network camera: a device that enables the reception, manipulation, storage and other processing, anywhere, of video information collected by a filming device permanently installed in a certain location, via wired/wireless Internet.

Chapter 2 Duties and Responsibilities of the Privacy Officer, etc.

Article 4 (Designation of the Privacy Officer)

The Company shall designate a Privacy Officer (Chief Privacy Officer, CPO) for the efficient performance of personal-information protection affairs. The Privacy Officer shall be the business owner or representative, and shall be in charge of the personal-information protection affairs of the Company.

Article 5 (Duties and Responsibilities of the Privacy Officer)

① The Privacy Officer shall perform the following duties for the protection of personal information:

1.Establishment and implementation of a plan for personal-information protection;

2.Receipt and handling of reports of personal-information infringement, such as loss, theft, leakage, alteration, or damage of personal information;

3.Verification and supervision of the management of personal information by persons handling personal information;

4.Verification and supervision of matters concerning protective measures, such as authority management for granting access privileges to personal information to persons handling personal information;

5.Compilation of statistics and materials related to personal-information protection;

6.Prevention and follow-up management of misuse and abuse of personal information;

7.Establishment and implementation of an education plan for personal-information protection;

8.Handling of complaints and provision of remedies for damage in connection with the processing of personal information;

9.Other matters which the Privacy Officer deems necessary for personal-information protection.

②The Privacy Officer may designate a “Personal Information Protection Department” to perform a supporting role in carrying out the duties, and may appoint the head of each department processing personal information as a “Personal Information Protection Manager by Field.”

Article 6 (Duties and Responsibilities of the Personal Information Protection Manager by Field)

The Personal Information Protection Manager by Field shall perform the following duties for the protection of personal information:

1.Verification and inspection of the status of processing of personal information in the relevant field;

2.Operation of the personal-information system of the relevant field and management of outsourced work;

3.Setting of user privileges for the relevant personal-information processing system;

4.Technical and managerial protective measures to ensure the safety of the relevant personal-information system;

5.Other duties necessary for personal-information protection.

Article 7 (Duties and Responsibilities of Persons Handling Personal Information)

Persons handling personal information by department shall perform the following duties for personal-information protection:

1.They shall destroy personal information with the approval of the Privacy Officer;

2.They shall perform the personal-information protection-related duties delegated by the Privacy Officer;

3.Where a person handling personal information becomes aware that infringement of personal information has occurred, that person shall report the same to the Privacy Officer and the Personal

Information Protection Manager by Field;

4.They shall perform duties related to the processing of personal information;

5.They shall comply with the internal management plan for personal information and the Personal Information Processing Policy;

6.They shall comply with the technical and managerial protective measures for personal information;

7.They shall conduct checks on illegal or improper personal-information infringement acts by employees of the relevant department or by third parties;

8.They shall comply with other matters necessary for personal-information protection.

Chapter 3 Protective Measures by Stage of Personal-Information Processing

Article 8 (Measures for Restricting Physical Access)

① Access to the location shall be restricted with respect to the data center and the area where data are stored; only persons authorized to enter by the Privacy Officer may enter, and a register of persons entering controlled areas shall be created and maintained.

② The Privacy Officer shall take protective measures by means of access control through physical locking devices, etc., for the safe storage of personal information and the personal-information processing system, including the following:

1.Where a person enters separate protective facilities prepared to prevent physical access or peruses personal information stored therein, the Privacy Officer shall ensure that a management ledger concerning the fact of entry and the contents of perusal by such person is prepared;

2.The Privacy Officer shall periodically review the entries and contents of perusal in the management ledger for physical-access restriction, check and verify whether there are any cases of entry or perusal without legitimate authority, and take necessary measures.

③ Access to the media shall be restricted with respect to USBs and other auxiliary storage media, and documents and files containing personal information; the Personal Information Protection Manager by Field shall store documents, auxiliary storage media, etc., containing personal information in a secure location equipped with locking devices.

Article 9 (Management and Authentication of Access Privileges)

① The personal information controller shall grant personal-information handling privileges to the personnel in charge to the minimum extent necessary for the performance of their duties, and shall grant differentiated access privileges (read/write/modify and delete) to personal information by task, by department, and by rank.

② Where the person handling personal information has been changed due to HR movements such as transfer or separation from employment, the personal information controller shall, without delay, change or terminate the access privileges to the personal-information processing system, including the following:

1.Upon HR movement, the existing access privileges shall be terminated at the system level as of the effective date of the HR order, and new privileges corresponding to the duties of the new department shall be newly registered;

2.Where a long-term leave of absence is taken in accordance with an HR order, all privileges of the person on leave shall be placed in dormant status at the system level as of the date of leave, and the dormant status shall be lifted as of the date of return when the person returns;

3.All system access privileges of a retiree shall be terminated in a batch as of the business day immediately following the date of separation.

③The personal information controller shall record the details concerning the granting, change, or

termination of access privileges, and shall comply with the retention period in accordance with the purpose of processing personal information, the retention period, and relevant statutes.

④ Where user accounts that can access the personal-information processing system are issued, a single unique user account (ID) shall be issued per person, and the user account shall not be shared with other persons handling personal information.

Article 10 (Encryption of Personal Information)

① The personal information controller shall encrypt and transmit/receive or store unique identification information, passwords and biometric information, credit card numbers, and account numbers, including the following:

1.Biometric information (fingerprints, iris, etc.) used for unique functions such as identification and authentication shall be stored after being encrypted so that it is not exposed or forged/altered;

2.Voice recordings stored during general (customer) consultations or general photographic information are excluded from the scope of encryption.

② Where the personal information controller transmits or receives the personal information set forth in paragraph (1) via information and communications networks or delivers such information through auxiliary storage media, etc., it shall encrypt the information in accordance with the following procedures:

1.A function whereby an SSL (Secure Socket Layer) certificate is installed on the web server so that information transmitted is encrypted in transmission/reception;

2.A function whereby an encryption application program is installed on the web server so that information transmitted is encrypted in transmission/reception.

③Where passwords are stored, they shall be stored after being subjected to one-way encryption so that they cannot be decrypted.

④ When persons handling personal information store the personal information set forth in paragraph (1) on a computer, they shall encrypt the information using commercial encryption software or safe encryption algorithms before storage.

Article 11 (Password Management)

The personal information controller shall establish and apply password composition rules as follows, so that persons handling personal information or data subjects can set and use safe passwords:

1.Frequency of change: change at least once every half-year;

2.Composition rules: composed of at least 12 digits combining three or more types from among uppercase English letters, lowercase English letters, numerals and special characters;

3.Restriction on use of identical passwords: not using ten or more passwords in rotation.

Article 12 (Access Control)

① In order to prevent unlawful access and intrusion incidents via information and communications networks, the personal information controller shall install an access control system that restricts the access privileges to the personal-information processing system by means of firewalls, etc., and restricts unauthorized access.

② Where a person handling personal information seeks to access the personal-information processing system from outside via information and communications networks, the controller shall apply secure access means such as a virtual private network (VPN) or a dedicated line.

③ The personal information controller shall take measures with respect to the personal-information processing system and business computers so that personal information being processed is not disclosed to a person without perusal privileges or leaked externally through the Internet homepage, shared-folder settings, etc.

Article 13 (Prevention of Forgery or Alteration of Access Records)

① For the prevention of forgery or alteration of access records, where a person handling personal information accesses the personal-information processing system and processes personal information (operations such as access to the database and input/output, modification, etc., of information on the database), the personal information controller shall retain and manage access records, including the time of processing and the details of processing, for at least six months.

② The personal information controller shall safely store the access records under paragraph (1) to prevent forgery or alteration.

Article 14 (Installation and Operation of Security Programs)

① The personal information controller shall install and operate security programs such as anti-virus programs, PC patch management systems, and PC personal-information protection systems to ensure that personal information is not lost, stolen, leaked, altered, or damaged:

1.It shall use the automatic update function of the security programs, or perform updates at least once a day;

2.Security programs such as anti-virus software shall be kept running at all times for real-time monitoring.

② Security programs shall be kept at the latest version, including through the automatic update function:

1.Where a warning concerning a malicious program has been issued, or where there has been a security-update notice from the manufacturer of the application or operating-system software in use, the corresponding update shall be immediately performed;

2.Security updates shall be set to occur automatically.

Article 15 (Frequency and Procedure of Internal Audits and Inspections)

① The Privacy Officer shall periodically audit or inspect whether the provisions prescribed by the laws and regulations relating to personal-information protection are being implemented.

② The Privacy Officer may establish a separate plan for the conduct of personal-information internal audits or inspections, including the subjects, procedures, and methods of such audits or inspections.

Article 16 (Reflection of Results of Internal Audits and Inspections)

① Where, as a result of an internal audit or inspection for personal-information protection, the Privacy Officer discovers problems in the management or operation of personal information or that a relevant employee has violated the contents of these Regulations, the Privacy Officer shall take necessary measures such as correction or improvement.

② Where corrective and improvement measures concerning facts of violation of personal-information protection have not been implemented, or where there is a concern that a serious impact on personal-information protection may arise, the Privacy Officer may take additional necessary measures, such as HR orders, against the relevant persons handling personal information, etc.

Article 17 (Fact-Finding Survey and Reflection of Results)

① Separately from internal or external audits relating to personal-information protection, the Privacy Officer may conduct fact-finding surveys on personal-information protection on a non-periodic basis.

② Where necessary, the Privacy Officer may establish and implement a separate fact-finding survey plan including the subjects, procedures, and methods of the survey.

③ Where, as a result of the fact-finding survey, the Privacy Officer discovers a violation of the contents of the internal management plan or any other problem in the management/operation of personal information, the Privacy Officer shall take corrective, improvement, or other necessary measures.

Chapter 4 Education on Personal-Information Protection

Article 18 (Establishment of an Education Plan for Personal-Information Protection)

① The Privacy Officer shall establish an education plan for personal-information protection and conduct education at least once a year (for at least one hour per session) for Personal Information Protection Managers by Field and persons handling personal information.

② After conducting personal-information protection education, the Privacy Officer shall review the outcomes of the education and the need for improvement, and shall reflect the same in the establishment of the education plan for the following year.

Article 19 (Implementation of Education on Personal-Information Protection)

① The Privacy Officer shall endeavor to raise the awareness of employees regarding the protection of the rights of data subjects, and shall conduct personal-information protection education periodically at least once a year (for at least one hour per session) in order to prevent the misuse/abuse or leakage of personal information.

② The education shall be conducted using various methods, such as classroom education and online education (e-learning), as well as the Internet, and may be entrusted to external specialized institutions where necessary.

③ Where there is an important matter to be disseminated regarding personal-information protection or where there are changes related to personal-information protection affairs, the Privacy Officer may conduct ad-hoc education through departmental meetings, etc.

④ The Personal Information Protection Manager by Field shall, before and after the education, attach supporting documents such as the education plan and the education results report and obtain the approval of the Privacy Officer, and shall retain such documents.

Chapter 5 Processing of Personal Information

Article 20 (Collection and Use of Personal Information)

① The personal information controller may collect personal information in any of the following cases, and shall use it within the scope of the purpose of such collection:

1.Where the consent of the data subject has been obtained;

2.Where there are special provisions in laws or where it is inevitable in order to comply with statutory obligations;

3.Where it is inevitable for the performance of the duties under the jurisdiction of public agencies as prescribed in statutes, etc.;

4.Where it is inevitable for the conclusion and performance of a contract with the data subject;

5.Where it is deemed manifestly necessary for the urgent benefit of the life, body, or property of the data subject or a third party, since the data subject or the legal representative of the data subject is in a state where it is impossible to express his/her will or the consent cannot be obtained due to unknown address, etc.;

6.Where it is necessary for achieving the legitimate interests of the personal information controller and such interests are manifestly superior to the rights of the data subject. In such case, only where it is substantially related to the legitimate interests of the personal information controller and does not exceed a reasonable scope;

7.Where it is urgently necessary for public safety and welfare, such as public health.

②Where the personal information controller obtains consent under paragraph (1) item 1, the personal information controller shall inform the data subject of the following matters. The same shall apply where any of the following matters is changed:

1.Purpose of collection and use of personal information;

2.Items of personal information to be collected;

3.Retention and use period of personal information;

4.The fact that the data subject has the right to refuse consent and, if any disadvantage arises from refusal of consent, the contents of such disadvantage.

Article 21 (Restriction on the Collection of Personal Information)

① Where the personal information controller collects personal information falling under any of the items of Article 20(1) of these Regulations, the controller shall collect the minimum personal information necessary for such purpose. In such case, the burden of proving the minimum collection of personal information shall be borne by the personal information controller.

② The personal information controller shall not refuse to provide goods or services to a data subject on the grounds that the data subject has not consented to the collection of personal information beyond the minimum necessary information.

Article 22 (Restrictions on the Processing of Sensitive Information and Unique Identification Information)

① The personal information controller shall not process sensitive information or unique identification information, except in any of the following cases:

1.Where the data subject is informed of the matters set forth in each item of Article 20(2) or each item of Article 23(2), and his/her consent is obtained separately from the consent to the processing of other personal information;

2.Where the processing of such personal information is required or permitted under statutes.

Article 23 (Provision of Personal Information)

① The personal information so collected may be provided to a third party in the following cases:

1.Where the consent of the data subject has been obtained;

2.Where personal information is provided within the scope of the purpose for which it was collected, in accordance with Article 20(1) items 2, 3, and 5 through 7 of these Regulations.

②When obtaining the consent under paragraph (1) item 1, the personal information controller shall inform the data subject of the following matters. The same shall apply where any of the following matters is changed:

1.Recipient of the personal information;

2.Purpose of use of the personal information by the recipient;

3.Items of personal information to be provided;

4.Retention and use period of the personal information by the recipient;

5.The fact that the data subject has the right to refuse consent and, if any disadvantage arises from refusal of consent, the contents of such disadvantage.

③ The personal information controller may provide personal information without the consent of the data subject, taking into account such matters as whether any disadvantage will arise to the data subject and whether necessary measures, including encryption, have been taken to ensure safety, within a scope reasonably related to the original purpose of collection, in accordance with Article 14-2(1) of the Enforcement Decree of the Personal Information Protection Act (or, if Article 14-2(1) of such Enforcement Decree is amended after the date of enactment of these Regulations, the amended provisions thereof).

Article 24 (Restrictions on the Collection, Use and Provision of Personal Information)

① The personal information controller shall not use personal information beyond the scope of the use purpose notified at the time of collection of personal information, or the scope under Articles 20 and 23 of these Regulations, nor provide personal information to a third party beyond the scope of such notification.

② Notwithstanding paragraph (1), the personal information controller may use personal information for purposes other than the original purpose or provide it to a third party in any of the following cases, except where there is a concern that it may unjustly infringe upon the interests of the data subject or a third party:

1.Where the data subject has given separate consent;

2.Where there are special provisions in other laws;

3.Where it is deemed manifestly necessary for the urgent benefit of the life, body, or property of the data subject or a third party, since the data subject or the legal representative of the data subject is in a state where it is impossible to express his/her will or the consent cannot be obtained due to unknown address, etc.;

4.Where personal information is provided in a form by which a specific individual cannot be identified, for such purposes as the compilation of statistics or academic research (information that may be used to identify a specific individual shall not be included in the information so provided);

5.Where it is impossible to perform the duties under the jurisdiction of the agency concerned, as prescribed by other laws, without using personal information for purposes other than the original purpose or providing it to a third party, and a deliberation/resolution by the Protection Commission under Article 7 of the Personal Information Protection Act has been undergone;

6.Where it is necessary to provide personal information to a foreign government or international organization for the implementation of a treaty or any other international agreement;

7.Where it is necessary for the investigation of a crime and the institution and maintenance of a prosecution;

8.Where it is necessary for the performance of the court's adjudication duties;

9.Where it is necessary for the execution of a punishment or for the execution of probation or protective disposition;

10.Where it is urgently necessary for public safety and welfare, such as public health.

③ When obtaining the consent under paragraph (2) item 1, the personal information controller shall inform the data subject of the following matters. The same shall apply where any of the following matters is changed:

1.Recipient of the personal information;

2.Purpose of use of the personal information (in the case of provision, the purpose of use of the recipient);

3.Items of personal information to be used or provided;

4.Retention and use period of the personal information (in the case of provision, the retention and use period of the recipient);

5.The fact that the data subject has the right to refuse consent and, if any disadvantage arises from refusal of consent, the contents of such disadvantage.

④Where the personal information controller provides personal information to a third party for purposes other than the original purpose pursuant to any of the items of paragraph (2), the personal information controller shall request the recipient of personal information to impose restrictions on the purpose and methods of use and other necessary matters, or to take necessary measures to ensure the safety of personal information. In such case, the person who has received such request shall take necessary measures to ensure the safety of personal information.

Article 25 (Restrictions on the Use and Provision of Personal Information so Received)

A person who has received personal information from the personal information controller shall not use the personal information for purposes other than the purpose for which the personal information was received, nor provide it to a third party, except in any of the following cases:

1.Where the data subject has given separate consent;

2.Where there are special provisions in other laws.

Article 26 (Processing of Personal Information following Outsourcing of Business)

① Where the personal information controller outsources the processing of personal information to a third party, it shall be done by means of a document containing the following:

1.Matters concerning the prohibition of the processing of personal information for any purpose other than the purpose of the outsourced work;

2.Matters concerning technical and managerial protective measures for personal information;

3.Other matters concerning the safe management of personal information, including the following matters as prescribed under Article 28 of the Enforcement Decree of the Personal Information Protection Act (or, if Article 28 of such Enforcement Decree is amended after the date of enactment of these Regulations, the amended provisions thereof):

- Matters concerning the restriction on sub-outsourcing;
- Matters concerning measures to ensure safety, such as restrictions on access to personal information;
- Matters concerning supervision, including inspection of the management status of personal information held in relation to the outsourced work;
- Matters concerning liability, including damages, in case the outsourcee (refer to the definition in paragraph (2)) violates the obligations to be complied with.

② Where the personal-information processing affairs are outsourced under paragraph (1), the contents of the outsourced work and the outsourcee (including any third party which is sub-outsourced from the person who has been outsourced to process personal information; hereinafter referred to as the “outsourcee”) shall be posted at a conspicuous location such as the Internet homepage so that the data subject may, at any time, easily confirm the same.

③ The Privacy Officer shall conduct appropriate supervision within the scope of the outsourced work as to whether the contents of paragraph (1) are faithfully implemented, so that the personal information processed under outsourcing can be safely managed.

Article 27 (Destruction of Personal Information)

① Where personal information has become unnecessary, such as upon the expiration of the retention period or the achievement of the purpose of the processing of personal information, the personal information shall be destroyed without delay. Provided that, where the personal information must be preserved pursuant to other statutes, the foregoing shall not apply.

② When destroying personal information pursuant to paragraph (1), measures shall be taken to ensure that the personal information cannot be restored or reproduced, as follows:

1.In the case of electronic files: permanently delete by methods that make restoration impossible;

2.In the case of records, printouts, documents, or other recording media other than those under item 1: shred or incinerate;

3.Deletion of records stored in a DB shall also constitute destruction.

③The personal information controller shall record and manage matters concerning the destruction of personal information in the personal-information destruction management ledger.

④ The implementation and verification of the destruction of personal information shall be carried out under the responsibility of the Privacy Officer.

⑤ The Privacy Officer shall verify the results of destruction after the implementation of the destruction

of personal information.

Article 28 (Posting of the Personal Information Processing Policy)

① The Privacy Officer shall establish a Personal Information Processing Policy containing the following matters and shall continuously post it on the Internet homepage so that data subjects can verify it:

1.Purpose of processing of personal information;

2.Processing and retention period of personal information;

3.Matters concerning the provision of personal information to third parties (only where applicable);

4.Matters concerning the outsourcing of the processing of personal information (only where applicable);

5.Matters concerning the rights and obligations of the data subject and his/her legal representative, and the methods of exercise thereof;

6.Items of personal information to be processed;

7.Matters concerning the destruction of personal information;

8.Matters concerning measures to ensure the safety of personal information;

9.Matters concerning the Privacy Officer;

10.Matters concerning changes to the Personal Information Processing Policy.

Chapter 6 Guarantee of the Rights of the Data Subject

Article 29 (Perusal, Correction/Deletion and Suspension of Processing of Personal Information)

① Where a data subject peruses personal information through an application to the Company, the person handling personal information shall follow the procedure below:

1.With respect to the data subject's request for perusal, verify that the requester is the person himself/herself and confirm the scope of personal information to be perused. In the case of an agent, verification shall be made by means of a power of attorney and a resident registration card or other identification document of both the principal and the agent. In the case of a legal representative, an additional document confirming the legal-representative status shall also be checked.

2.Verify the restrictions on the perusal, correction/deletion and suspension of processing of personal information under Article 35 of the Personal Information Protection Act and Article 30 of these Regulations. 3. In the case of restriction, postponement, or refusal of perusal, the relevant data subject shall be notified, within ten (10) days from the date of receipt of the request for perusal, of the reason for postponement or refusal and the method of objection, by means of the Notice of Postponement/Refusal of Perusal [Annexed Form No. 9] prescribed in the "Public Notice on the Methods of Processing Personal Information."

3.Allow the data subject to peruse the personal information.

②Where a data subject requests the correction, deletion or suspension of processing of personal information through an application to the Company, the person handling personal information shall follow the procedure below:

1.Verify that the requester for correction, deletion or suspension of processing is the person himself/herself, and confirm the scope of personal information for which correction, deletion or suspension of processing is requested. In the case of an agent, verification shall be made by means of a power of attorney and a resident registration card or other identification document of both the principal and the agent. In the case of a legal representative, an additional document confirming the legal-representative status shall also be checked.

2.Verify the restrictions on the correction, deletion or suspension of processing of personal information under Article 36 of the Personal Information Protection Act and Article 30 of these

Regulations, including the following:

- Where other laws specify the personal information as the subject of collection, deletion thereof may not be requested. In such case, the personal information controller shall, without delay, notify the data subject of such fact.
- Where the personal information controller receives a request from the data subject, the personal information controller shall, except where a special procedure is provided in other statutes, investigate the personal information without delay, take necessary measures such as correction or deletion in accordance with the data subject's request, and notify the data subject of the results. Where necessary in the course of investigation, the personal information controller may have the data subject submit evidentiary materials necessary to confirm the contents of the request for correction or deletion.
- Where the personal information controller deletes personal information, it shall take measures so that the information cannot be restored or reproduced.

3.In the case of refusal of correction, deletion or suspension of processing of personal information, the relevant data subject shall be notified, within ten (10) days from the date of receipt of the request, of the reason for refusal and the method of objection, by means of the Notice of Results in Response to Requests for Correction, Deletion or Suspension of Processing [Annexed Form No. 10] prescribed in the "Public Notice on the Methods of Processing Personal Information."

4.The person handling personal information shall modify the matters of correction, deletion, or suspension of processing of personal information in accordance with the data subject's request.

③Procedures for objection in response to a data subject's request for perusal, correction/deletion, or suspension of processing of personal information shall be governed by the Company's separately prescribed "Personal Information Processing Policy."

Article 30 (Restrictions on Perusal, Correction/Deletion, and Suspension of Processing of Personal Information)

① The personal information controller may notify the data subject of the reason and restrict or refuse perusal in any of the following cases:

1.Where perusal is prohibited or restricted by statute;

2.Where there is a risk of harm to the life or body of another person, or of unjust infringement on the property and other interests of another person;

3.Where the performance of any of the following duties is seriously impeded:

②Affairs concerning the imposition, collection or refund of taxes;

③ Affairs concerning examinations relating to academic qualifications, skills and recruitment, and qualifications screening;

④ Affairs concerning audits and investigations currently in progress under other statutes;

⑤ Other cases prescribed by law.

⑥ A data subject may not request the deletion of personal information where it is specified as a subject of collection under other statutes.

⑦ The personal information controller may refuse a data subject's request for suspension of processing in any of the following cases:

1.Where there are special provisions in laws or where it is inevitable in order to comply with statutory obligations;

2.Where there is a risk of harm to the life or body of another person or of unjust infringement on the property and other interests of another person;

3.Where the performance of a contract with the data subject, such as the provision of the agreed services, would be difficult unless personal information is processed, and the data subject has not clearly expressed an intention to terminate such contract.

⑧Where the personal information controller intends to postpone or refuse a data subject's request for perusal, correction/deletion, or suspension of processing of personal information pursuant to paragraphs (1), (2), and (3), the personal information controller shall, within ten (10) days from the date of receipt of the request pursuant to Article 29 or 30 of these Regulations, notify the relevant data subject of the reason and the method of objection by means of the Notice of Postponement/Refusal of Perusal.

Article 31 (Response in Case of Leakage of Personal Information)

① Where the Company becomes aware that personal information has been leaked, the Company shall, without delay, report the same to the Privacy Officer, and shall promptly take the following measures:

- Identify the items of personal information leaked, the time and circumstances of leakage, and measures to minimize damage;
- Maintain records of the facts of leakage and the response measures;
- Strengthen internal inspections and technical/managerial measures to prevent recurrence.

② Where the personal information leaked involves 1,000 or more data subjects, the Company shall, in accordance with Article 34 of the "Personal Information Protection Act" and Article 39 of the Enforcement Decree of the same Act, report the same to the following agencies within 72 hours from the time it becomes aware of the relevant fact:

- Receiving body: Personal Information Protection Commission (https://www.privacy.go.kr) or Korea Internet & Security Agency (https://privacy.kisa.or.kr/wrap/main.do);
- Submission form: Personal Information Leakage Report.

③ Where the fact of leakage has been confirmed, the Company shall individually notify the data subjects of the following matters in accordance with the relevant statutes. Provided that, where individual notification is difficult, the Company may substitute this with a notice on the homepage or by other appropriate means:

- Items of personal information leaked;
- Time and circumstances of leakage;
- Response measures of the Company and means of minimizing damage;
- Methods of response and reporting procedures available to the data subject.

④ The Company shall implement personal-information leakage response procedures in accordance with a separate leakage response manual or information-security guideline, and shall comply with the relevant statutes and the guidelines of the supervisory authority.

Article 32 (Prevention of Infringement of Personal Information)

The personal information controller shall take managerial and technical measures so that personal information is not leaked externally or infringed, and persons handling personal information shall comply with related matters.

Article 33 (Provisions Applied Mutatis Mutandis)

Matters concerning the processing and protection of personal information not prescribed in these Regulations shall be governed mutatis mutandis by the "Personal Information Protection Act" or the "Personal Information Protection Guidelines" of the Ministry of Health and Welfare.

[별지 제9호 서식]

개인정보 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절) 통지서

(앞 쪽)

수신자 (우편번호: , 주소:)

요구 내용						
열람 일시		열람 장소				
통지 내용 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절)						
열람 형태 및 방법	열람 형태	[ ]열람·시청	[ ]사본·출력물	[ ]전자파일	[ ]복제물·인화물	[ ]기타
	열람 방법	[ ]직접방문	[ ]우편	[ ]팩스	[ ]전자우편	[ ]기타
납부 금액	①수수료 권	②우송료 권	계(①+②) 권			
	수수료 산정 명세					
사 유						
이의제기방법	※ 개인정보처리자는 이의제기방법을 적습니다.					

「개인정보 보호법」 제35조제3항·제4항 또는 제5항과 같은 법 시행령 제41조제5항 또는 제42조제2항에 따라 귀하의 개인정보 열람 요구에 대하여 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

210㎜×297㎜[신문용지 54g/㎡]

(뒤 쪽)

유의사항

1. 개인정보 열람 장소에 오실 때에는 이 통지서를 지참하셔야 하며, 요구인 본인 또는 그 정당한 대리인임을 확인하기 위하여 다음의 구분에 따른 증명서를 지참하셔야 합니다.

   가. 요구인 본인에게 공개할 때: 요구인의 신원을 확인할 수 있는 신분증명서(주민등록증 등)

   나. 요구인의 대리인에게 공개할 때: 대리인임을 증명할 수 있는 서류와 대리인의 신원을 확인할 수 있는 신분증명서

2. 수수료 또는 우송료는 다음의 구분에 따른 방법으로 냅니다.

   가. 국가기관인 개인정보처리자에게 내는 경우: 수입인지

   나. 지방자치단체인 개인정보처리자에게 내는 경우: 수입증지

   다. 국가기관 및 지방자치단체 외의 개인정보처리자에게 내는 경우: 해당 개인정보처리자가 정하는 방법

   ※ 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속 기관 또는 지방자치단체인 개인정보처리자에게 수수료 또는 우송료를 내는 경우에는 「전자금융거래법」 제2조제11호에 따른 전자지금수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 낼 수 있습니다.

3. 열람제한, 열람연기 또는 열람거절의 통지를 받은 경우에는 개인정보처리자가 이의제기방법란에 적은 방법으로 이의제기를 할 수 있습니다.

210㎜×297㎜[신문용지 54g/㎡]

[별지 제10호 서식]

개인정보 ([ ] 정정·삭제, [ ] 처리정지) 요구에 대한 결과 통지서

수신자 (우편번호: , 주소:)

요구 내용	
□ 정정·삭제 □ 처리정지 조치 내용	
□ 정정·삭제 □ 처리정지 결정 사유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.

「개인정보 보호법」 제36조제6항 및 같은 법 시행령 제43조제3항 또는 같은 법 제37조제6항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

유의사항

개인정보의 정정·삭제 또는 처리정지 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.

210㎜×297㎜[신문용지 54g/㎡]