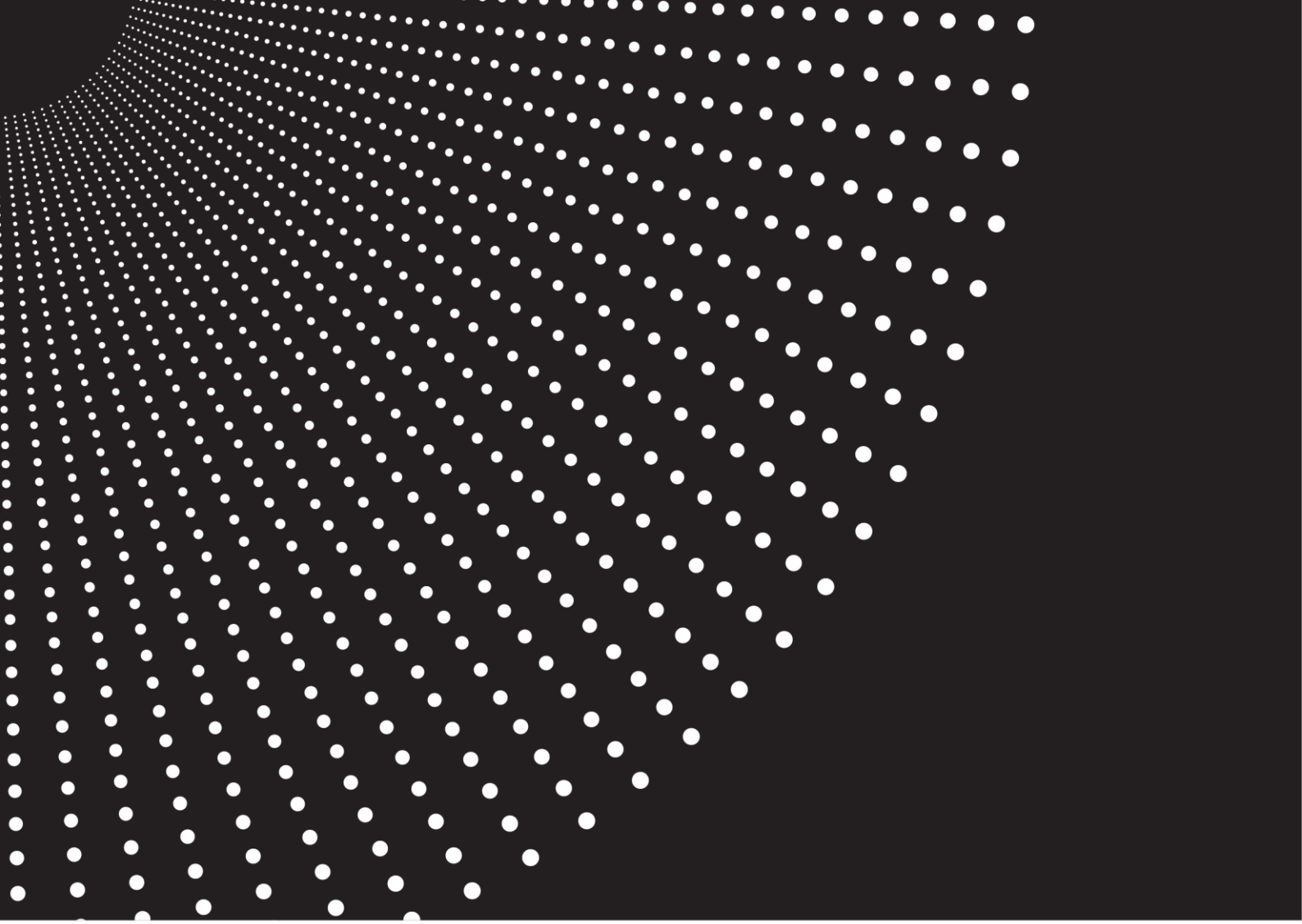

Privacy Policy on Processing of Personal Information

MACQUARIE

Contents

Macquarie Korea Asset Management Co., Ltd (the Company) has a Privacy Policy on Processing of Personal Information (this Privacy Policy) as follows in an effort to protect the personal information and rights of the principal of information (Data Subject) and to smoothly address the grievance suffered by the Data Subject related to the personal information pursuant to Article 30 of the Personal Information Protection Act (PIPA). The group-wide Macquarie Group Privacy Policy is supplemental to this Policy and should therefore be read together.

Article 1 (Purpose of Processing Personal Information)

The Company processes personal information for the purposes described in each of the following sections. The processed personal information will not be used for any other purposes than as set out below. Unless otherwise permitted by relevant law, the Company will notify and where required obtain prior consent from Data Subjects in case of any changes to the following purposes of use.

In the case of personal information of family members of employees, the minimum personal information which is necessary for the provision of family welfare benefits may be collected without consent in accordance with Article 48 of the Labor Standards Act (in the case of resident registration numbers, it can only be collected when there is a specific basis for laws and regulations).

On the other hand, in principle, the Company does not process the personal information of children under the age of 14. As an exception, if the processing of the personal information of a child under the age of 14 is necessary to provide welfare benefits to the family of an employee, and separate consent is required, the personal information of the child will be processed within the minimum necessary scope with the consent of the employee who is the legal representative of the child in accordance with Article 22-2 of the Personal Information Protection Act and other relevant laws.

1. Management of Officers and Employees (related to the collection of information of officers and employees)

[General Personal Information]

(1) Mandatory Information

- Personnel Management: recruitment, retirement, promotion, performance evaluation, remuneration, rewards and sanctions, relocation, secondment, transfer, etc.
- Career Management: Issuance of certificates regarding employment including certificate of employment, certificate of career or certificate of retirement and verification of relevant facts
- Wage Management: Base salary, profit share, other compensation, allowance, retirement pension, etc.
- Employee Benefits: Group life and medical insurance, medical aid, vehicle support, corporate housing, provision of loan, vacation, etc.
- Tax/Insurance: Subscription to legally required insurance policies including the major public insurances; payment and deduction of taxes including income tax
- Compliance/Performance of contract: Performance of employment contract, compliance with any and all internal and/or Macquarie Group policies, fair treatment and provision of opportunities among employees, confirmation and management of persons subject to veterans compensation, performance of legal and administrative obligations required of the Company including under industrial security and health laws, foreign worker laws, financial laws and related regulations

- Security/Contact: Protection of information processed by the Company, maintenance, improvement and monitoring of security system, prevention of unfair and illegal activities which may occur within the Company and collection of evidence, sharing of contact information and establishment of emergency contact network, etc.
- Marketing: Provision of contact information to customers or other third parties for marketing or business purposes
- Compliance with Foreign Laws: Overseas affiliates' compliance with foreign laws and cooperation with overseas regulators for their supervision

(2) Optional Information

- Provision of welfare to officers and employees

[Personally Identifiable Information]

(1) Mandatory Information

- Identification and verification of the individual, provision of welfare benefits such as enrollment in various insurances, and tax-related work such as income tax withholding

(2) Optional Information

- Support for transportation necessary for work, support for overseas business trips

[Sensitive Information]

(1) Mandatory Information

- Personnel management, improvement of work environment, medical checkup and medical support, prevention of crimes and corruption that may occur within the company, and collection of evidence

(2) Optional Information

- Understand Macquarie Human Resources and identify and support opportunities to promote diversity and inclusion

2. Transactions with customers (related to the collection of information of officers and employees of corporate customers or counterparties, and counterparties)

- Determination of whether to establish (financial) transaction, and establishment, maintenance, performance, and management of the (financial) transactional relationship, etc.
- Investigation of financial incident, settlement of dispute, handling of complaints, etc.

Article 2 (Items of Personal Information to be Processed)

① The items of personal information to be processed and method of collection thereof in order for the Company to attain the purposes set forth in Article 1 are as follows:

1. In case of Officers and Employees

[General Personal Information]

(1) Mandatory Information

- Name, photo, date of birth, address, home telephone number, mobile phone number, e-mail, gender, military service information, place of birth, nationality, family members (including family relations, name, age, occupation, co-habitancy, resident registration number of family members), emergency contact, etc.
- Educational background (college/university, location, major, year of entrance and year of graduation, graduation, GPA, etc.), work experience (employer, title, responsible area, service period), qualifications, history of awards / disciplinary actions, dates of employment, department, title, duties, etc.
- E-mails received and sent via Company e-mail account, telephone conversation via office telephone and instant messenger communications via the Company's communication network
- Office access records, logon records, work attitude, performance results, evaluation of customer relationship
- Video clips collected through CCTV

(2) Optional Information

- Veterans compensation information, location of registration, vehicle registration number, cultural background, responsibilities for care

[Personally Identifiable Information]

(1) Mandatory Information

- Resident Registration Number (Social Security Number), Alien Registration Number

(2) Optional Information

- Driver's license number, passport number

[Sensitive Information]

(1) Mandatory Information

- Health-related information, criminal convictions
- E-mails sent and received through the company's e-mail account, calls made using the company's telephone, and messengers through the company's network

(2) Optional Information

- Sexual orientation, gender awareness, disability

2. In case of Officers and Employees of Corporate Customers or Counterparties, and Counterparties

(1) Minimum personal information required to conduct business according to Article 1.2.

② In principle, the Company does not collect sensitive information that may threaten to infringe upon the privacy of the Data Subject. If necessary, the Company collects sensitive information by obtaining additional consent of the Data Subject and uses the same only for the limited purposes so consented; provided, however, that the Company checks the accuracy and currency of the sensitive information on a regular basis.

③ Employee information is collected as needed on an ongoing basis through various means such as webpages, interviews, written documents, faxes, phone calls, emails, and information collection programs. On the other hand, the personal information of corporate customers or counterparties' employees is collected on the premise that the corporate customer or counterparty lawfully provides such information. This information is gathered through various methods, including business cards, transaction documents, working group lists, and other written materials, as well as phone calls and emails.

Article 3 (Period of Process and Retention of Personal Information)

① The personal (credit) information of the Data Subject collected for the purposes described in Article 1 will be retained and used until the above stated purposes of provision are all accomplished. The concerned personal (credit) information will be destroyed when it is confirmed to be unnecessary unless there exists an obligation to retain it pursuant to the laws and regulations.

② On the other hand, if the retention of personal information is required by other laws and regulations, including the following cases, the personal information will be safely retained in accordance with the relevant laws and regulations, and the personal information will never be used for any other purpose.

(1) Information required for issuance of career certificate under the Labor Standards Act (Article 39 of the Labor Standards Act and Article 19 of the Enforcement Decree of the same Act): 3 years, Important documents related to the list of employees and employment contract (Article 42 of the Labor Standards Act): 3 years
(2) Medical Examination Report of Incumbents (Article 164, Paragraph 1 of the Occupational Safety and Health Act): 3 years
(3) Books and documentary evidence related to all transactions (Article 85-3 of the Framework Act on National Taxes), and important documents related to corporate book-keeping (Article 112 of the Corporate Income Tax Act): 5 years
(4) Under the Commercial Act, commercial books and important documents related to business: 10 years, slips or similar documents: 5 years

③ In the case of employee information, it is retained for 10 years from the end of the employment contract in accordance with the Macquarie retention period.

Article 4 (Provision of Personal Information to a Third Party)

① In principle, the Company will process the Data Subject's personal information within the scope of the purpose outlined in Article 1 and will not process information exceeding the primary scope or provide it to a third party without the consent of the Data Subject in advance. However, in any of the following cases, except where there is a concern of unfairly infringing upon the interests of the Data Subject or a third party, the personal information may be used for other purposes or provided to a third party.

1. When the Data Subject has agreed on the provision and disclosure of information to a third party in advance
2. When there are special provisions in other laws

3. When the personal information is clearly acknowledged as necessary for the purpose of urgency in life, body or property profits for the Data Subject or a third party
4. When it is urgently necessary for public safety and well-being, such as public health

② The Company provides the personal information of its employees as follows.

Recipient	Recipient's Purpose of Use	Items To Be Provided	Period of Retention and Use by Recipient
Financial Services Commission, Financial Supervisory Services, Korea Financial Investment Association	Supervision of compliance with local laws and regulations; regulatory reporting; periodic and extraordinary audits; professional license management, etc.	Those personal information items collected by the Company to the minimum extent necessary to achieve the purpose of use	Until the purpose of use is fully achieved

Article 5 (Delegation of Personal Information Processing Services)

① The Company may delegate the processing of personal information in the following cases.

Recipient	Recipient's Purpose of Use
Macquarie Securities Korea Limited	HR support
Kyobo Life Insurance Shinhan Bank Mirae Asset Securities	Provision and administration of retirement pension services and tax reporting to National Tax Service.
KMI, Kangbuk Samsung Hospital (Medical check-up center)	Medical check-up service

② When executing a service (outsourcing) agreement, the Company clearly sets forth the compliance with personal information protection related laws, the prohibition of provision of personal information to a third party, and where the responsibility lies, and maintains the terms and conditions of the service agreement both in writing and in electronic form. The Company will notify any changes to the service providers by email, posting on the internet homepage or by amending and publishing this Privacy Policy.

Article 6 (Overseas Transfer of Personal Information (including Provision, Inquiry, Delegation of Processing, and Retention)

① The Company may transfer the personal information of its employees outside of the Republic of Korea with the consent of the employees. Employees have the right to refuse the transfer of their personal information overseas by either not providing consent or by notifying the company separately of their refusal.

② The Company may entrust the processing of personal information as outlined below for transactions with customers or counterparties as specified in Article 1, Paragraph 2.

Personal information items	Country, Period and Method	Name (Contact details)	Purpose of Use and Retention/Usage Period	Relevant Legal Provisions
Name, date of birth, address, contact details, occupation	The UK and India Before transaction with customers or counterparties Salesforce	KPMG LLP, KPMG Global Services Pvt Ltd. (Helena.Bartles@kpmg.co.uk)	Limited to the Purpose of onboarding support services for compliance with Anti-Money Laundering laws, relevant regulations and policies The period specified by relevant laws, regulations and policies	Article 28-8, Paragraph 1, Subparagraph 3 of the Personal Information Protection Act

③ The Data Subject referred to in Paragraph 2 may refuse the transfer of their personal information overseas by either not providing consent or by notifying the company separately of their refusal. However, in such cases, the initiation and maintenance of (financial) transactional relationships will not be possible.

Article 7 (Rights and Obligation of Data Subject and Method of Exercise)

① The Data Subject may exercise rights related to the protection of personal information, such as access, transfer, correction and deletion, suspension of processing, withdrawal of consent to the processing of personal information, and refusal or explanation of automated decisions to the Company in accordance with relevant laws and regulations, including the Personal Information Protection Act.

② The Data Subject who inspected his/her own personal information may request the Company to correct or delete his/her personal information that are not verifiable or inconsistent with the facts. However, in cases where such personal information is stipulated to be collected in other laws and regulations, the Data Subject may not request the deletion of such information.

③ The Data Subject may request the Company to suspend the processing of his/her own personal information. However, in any of the following cases, the Company may refuse such request after notifying the Data Subject of the reason of such refusal:

1. If there is a special provision in laws or it is inevitable to refuse such request to comply with its obligations under applicable laws or regulations

2. If such an act will likely inflict damages upon another person's life or body or unfairly infringe upon another person's properties and other interests

3. If it is difficult to carry out any contract due to failure in providing services agreed with the Data Subject or otherwise, unless relevant personal information is processed, but the Data Subject has not expressly expressed his/her intention of termination of such contract.

④ The exercise of rights pursuant to Paragraph 1 may also be done through the legal representative of the Data Subject or a person authorized by the Data Subject, merely, In this case, the employee shall submit a power of attorney to the Company in accordance with the notice on how to process personal information.

⑤ The Company will take measures without delay in accordance with relevant laws such as the Personal Information Protection Act regarding the exercise of the rights of Data Subject.

Article 8 (Destruction of Personal Information)

① In principle, when the personal information becomes unnecessary, such as the expiration of the retention period of the personal information, the achievement of the purpose of processing the personal information, or the expiration of the processing period of pseudonymous information, the Company destroys the personal information without delay unless it is required to be retained in accordance with other laws and regulations.

② If the Company is required to retain personal information without destroying it, the Company shall store and manage the personal information or personal information file separately from other personal information.

③ Any printout, document, etc. containing personal information will be destroyed by incinerating or shredding them into pieces, and personal information in the form of electronic file will be destroyed by permanently deleting it in an irrevocable manner.

④ The Company selects the personal information for which the reason for destruction has occurred and destroys the personal information with the approval of the Company's Privacy Officer.

Article 9 (Measures to Ensure Safety of Personal Information)

The Company takes following technical, administrative and physical actions required to ensure the safety of personal information in accordance with Article 29 of the PIPA:

1. Minimizing the number of employees to handle personal information and providing training

   The Company designates employees to handle personal information and implements measures to minimize the number of employees to manage personal information.

2. Conducting regular self-checks

   The Company conducts regular inspections of user access to Sharepoint/Sharedrive, where personal information is stored, in order to ensure the stability of the processing of personal information.

3. Establishment and implementation of internal management plan

   The Company may establish and implement an internal management plan if necessary for the safe processing of personal information.

4. Encryption of personal information

   Users' passwords, biometric information, and other related personal information deemed necessary are stored and managed in an encrypted manner. Data files containing personal information are to be encrypted or locked before being sent electronically.

5. Technical measures against hacking, etc.

   The Company installs and periodically updates and inspects security programs to prevent the leakage of and damage to personal information due to hacking or computer viruses, etc. Further, the Company installs security systems and technically/physically monitors and blocks the restricted area.

6. Access control to personal information

   The Company takes necessary measures to control the access to personal information by granting, changing and cancelling the right to access the data base system in which personal information is

processed, and also controls unauthorized access from the outside by using adequate IT security systems described in item 5 above.

7. Retention of access logs and prevention of forgery and alteration

   The Company shall retain and manage access logs to key personal information processing systems for at least 3 years, and shall adopt security functions to prevent forgery, alteration or loss of access logs.

8. Use of locking system for document security

   The Company keeps the documents, auxiliary storage medium, etc. containing personal information in a safe place with locking system.

9. Access control for unauthorized persons

   The Company has secured physical locations to keep personal information and establishes and operates the access control process for such locations.

Article 10 (Privacy Officer)

In order to protect personal information and deal with complaints about personal information, the Company has designated a Compliance Officer (Young Ju Ahn, contact number: 02-3705-4950) as Privacy Officer under Article 31(1) of the Personal Information Protection Act.

Article 11 (Installation and Operation of Visual Data Processing Devices (Closed Circuit Television, "CCTV"))

The Company installs and operates Visual Data Processing Devices as follows.

① Grounds and Purposes for Installation of Visual Data Processing Devices
- Facility safety, crime prevention, collection of evidence, security of safe etc. for the Company

② Number of processors installed, location of installation, scope of filming
- Location and number of installed processors: one each CCTV on the ceiling around the safe in the company's two office spaces and common areas such as lobby and corridors of the office building of the Company
- Scope of filming: entire space of the safe and major facilities

③ Responsible manager and department and persons having access to the imagery information
- Responsible manager and department: Manager of Business Services Department (refers to the manager of the Business Services Department of Macquarie Securities Korea Limited, an affiliated company, which provides general affairs services such as facility management in accordance with the service agreement

signed)
- Persons having access to the imagery information: Business Services Department Manager and Privacy Officer or persons who are authorized by the Privacy Officer

④ Imagery information filming hours, retention period and place, and processing method
- Filming hours: 24 hours
- Retention period: 30 days from filming, 30 days for the essential area (data center, main entrance)
- Retention place and processing method: retained and processed in the data centre operated by Business Services Department

⑤ Method and place for inspection of imagery information
- Method: request to the manager described in Item 3. above

⑥ Measures in response to the request of the Data Subject for inspection, etc. of imagery information
- In order for the Data Subject to access imagery information, he/she shall file an application for access with the Company in a form of application for inspection/confirmation of existence of the personal imagery information. The Company allows access to the imagery information only when the Data Subject himself/herself is filmed, or when it is explicitly required for benefit in life, body, and asset of the Data Subject.

⑦ Technical, managerial and physical measures for protection of imagery information
- For protecting imagery information, the Company takes actions including maintaining an internal management plan, control of access and restriction of accessing authority, safe storing of the imagery information, application of transfer technology, storing of processing records and measures for preventing forgery or alteration, preparation of storage facility and installation of lock.

Article 12 (Amendment to this Privacy Policy)

This Privacy Policy will apply from the enforcement date set out below. Any addition, deletion and correction of this Privacy Policy made pursuant to applicable laws and regulations will be notified in accordance with the method prescribed by the relevant laws and regulations.

Article 13 (Remedy for Infringement of Rights)

If the Data Subject needs to file a report or receive counseling with respect to the infringement of personal information, the Data Subject may contact the following organizations:

1. Personal Information Dispute Mediation Committee

(https://www.kopico.go.kr/ (without area code) 1833-6972)

2. Privacy Invasion Report Center in the Korea Internet Security Agency

(https://privacy.kisa.or.kr/ (without area code) 118)

3. Supreme Prosecutors' Office (www.spo.go.kr/ (without area code) 1301)
4. National Police Agency (ecrm.cyber.go.kr/ (without area code) 182)

Addendum (August 24, 2012)

This Privacy Policy on Processing of Personal Information shall take effect from the date of the resolution of the Board of Directors.

Addendum (June 24, 2014)

This policy shall take effect as of June 24, 2014.

Addendum (October 31, 2016)

This policy shall take effect as of October 31, 2016.

Addendum (September 25, 2020)

This policy shall take effect as of September 25, 2020.

Addendum (October 24, 2024)

This policy shall take effect as of October 24, 2024.

Addendum (September 23, 2025)

This policy shall take effect as of September 23, 2025.