CJ GLOBAL PRIVACY POLICY

Table of Contents

1. INTRODUCTION

OVERVIEW

In the process of conducting our business activities, we process Personal Information from various Data Subjects, including our customers and employees. Because such Personal Information is valued data entrusted to CJ, we have established the "CJ Global Personal Information Protection Policy" (hereinafter "this Policy") to protect and safely manage this information.

Because this Policy is a set of detailed guidelines to fulfill the Personal Information protection commitment declared in the 〈CJ Code of Business Conduct〉, we present the general principles and minimum standards that all CJ members must follow in order to ensure the rights of the Data Subjects and safely process the Personal Information while complying with the Personal Information protection laws of the communities and countries in which we do business.

If you wish to establish additional guidelines by country or industry beyond this Policy, the fundamental principles of such guidelines must be consistent with this Policy. Any specific details of the guidelines shall follow the regulations of each country.

SCOPE AND WORLDWIDE APPLICATION

This Policy applies to everyone working for CJ all over the world no matter the location, role, or position. Regardless of the type of employee, whether regular or contract, this Policy applies to all employees, middle managers, executives, directors, committee members, and advisers (hereinafter "**CJ members**").

Also, regardless of the title of consultant, agent, intermediary, representative, etc., this Policy or policies substantially equivalent to this Policy must be followed by all third parties representing or working on behalf of CJ.

COMPLIANCE WITH APPLICABLE LAW

CJ members must not only abide by the regulations of the communities or countries in which CJ does business, but also the regulations of the countries of the Data Subjects. Also, CJ members must always be mindful of Personal Information protection regulations of other important countries. Widely known Personal Information protection regulations include the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Chinese Law on the Protection of Consumer Rights and Interests, and the Chinese Cyber Security Law, but are not limited to such regulations.

CJ Members should be particularly cautious as their actions could be subject to extraterritorial

application of those countries' Personal Information protection regulations such as GDPR and CCPA.

If the Personal Information protection regulations of the communities and countries in which CJ conducts business conflict or require stricter compliance than that of this Policy, the regulations of the relevant countries take priority. This Policy must be followed even if any community or country does not have Personal Information protection regulations, and please note that any breach of this Policy is not justified because it corresponds with the practices of any community or country. This is because if Personal Information is infringed upon or divulged, regardless of how small, it can lead to serious consequences, damage to reputation, loss of trust, and legal liability to CJ and CJ members.

2. DEFINITIONS

A. "CJ" refers to the CJ Corporation, its subsidiaries, and its affiliates domestically and internationally.

B. "Personal Information" refers to all information related to identified or identifiable natural individuals. Such information includes directly or indirectly identifiable names, identification numbers, location information, and *online identifiers*, along with the physical, physiological, psychological, financial, cultural, and social identity of the natural individual that can be identified through one or more specific factors. However, the definition and scope of the personal information according to the regulations may defer by country.

   * *Online Identifiers: Refers to identifiers and other information in along with personally identifiable information, and includes IP addresses, MAC addresses, online cookie IDs, RFIDs, etc.*

C. "Personal Information Processing" refers to actions including the collection, creation, connection, linkage, recording, saving, retention, manufacturing, editing, searching, output, correction, recovery, utilization, provision, disclosure, destruction, and other similar actions regarding Personal Information.

D. "Data Subject" refers to a natural individual that can be recognized by the processed information, which means that the natural individual is the subject of the information.

E. "Anonymization" refers to processing or other methods of making the information no longer able to identify the Data Subject.

F. "Pseudonymization" refers to deleting a part or replacing a part or all of the Personal Information so that it cannot identify the unique individual without additional information.

G. "Outsourcing Personal Information Processing" refers to entrusting a third party with processing the Personal Information of Data Subjects for CJ's business purposes.

H. "Cross-border Transfer of Personal Information" may include Personal Information transferred

across borders and collected and stored directly in overseas systems, Personal Information transferred to overseas systems through data linkage, Personal Information accessible remotely from overseas, or Personal Information included when sending an electronic file.

3. CJ'S PRIVACY PRINCIPLES

LAWFULNESS, FAIRNESS, AND TRANSPARENCY

CJ members must process Personal Information lawfully, fairly, and transparently. Transparency means clearly showing the sequence of actions when processing Personal Information in an open way that is easy to understand and easily accessible to the Data Subject.

PURPOSE LIMITATION

CJ members must specifically and clearly inform the Data Subject of the purpose of collecting Personal Information, and the Personal Information must be collected for legitimate purposes. Also, the Personal Information, in principle, must only be used within the scope of the purpose of collection.

DATA MINIMIZATION

CJ members must only collect Personal Information within the scope that is appropriate, reasonable, and necessary for processing Personal Information.

ACCURACY

CJ members must process Personal Information accurately without error, and if the Data Subject requests that incorrect information be deleted or corrected, CJ members must take reasonable measures for this.

STORAGE LIMITATION

CJ members must only store the Personal Information as long as necessary for the purpose of processing Personal Information, and Personal Information that is past the purpose of processing must be destroyed or anonymized.

INTEGRITY AND CONFIDENTIALITY

CJ members must protect Personal Information from unauthorized processing, illegal processing,

accidental loss or damage, destruction, or injury through reasonable managerial and technical measures.

ACCOUNTABILITY

All CJ members must observe and implement the above principles related to Personal Information protection, and take all necessary measures to ensure credibility to the Data Subject.

4. COLLECTING PERSONAL INFORMATION

COLLECTING THE MINIMUM NECESSARY PERSONAL INFORMATION

When collecting Personal Information, it is our standard that CJ only collects the minimum Personal Information necessary to perform the essential functions of the service at the required time. You must not refuse to provide services because the Data Subject does not agree to the collection of Personal Information other than the minimum necessary.

Also, in case the purpose of collecting the Personal Information can be achieved if it is processed anonymously or pseudonymously, then it must be anonymized if possible and if the purpose cannot be achieved with Anonymization, then it must be pseudonymized.

LEGALITY OF PERSONAL INFORMATION COLLECTION

When collecting Personal Information, we must carefully check not only the regulations of the countries where CJ does business, but also the countries to which the Data Subject for collecting Personal Information belongs, and the Personal Information must be collected in compliance with such legal requirements and procedures.

In most countries, the legality of Personal Information collection is recognized when express consent is obtained from the Data Subject. To be recognized as legal consent for the collection of Personal Information, you must obtain consent based on the free will of the Data Subject, and you must follow the legally required procedures, such as informing the Data Subject of the notifications pursuant to regulations.

On one hand, the California CCPA and regulations from some jurisdictions only require prior notice and disclosure of the collected Personal Information for data collection, and the ability to opt-out. Besides these, each jurisdiction may have different requirements for recognizing the legality of Personal Information collection, such as when necessary for the conclusion and execution of contracts with Data Subjects.

Also, processing certain Personal Information that may significantly infringe on religion, political disposition, medical records, genetics, race or ethnicity, biometric information, and other areas of private life must be minimized as much as possible. Some countries may require a separate consent procedure to collect such Personal Information, and others may prohibit processing certain Personal Information, such as criminal backgrounds. Therefore, always check the regulations of your country or local jurisdiction.

If you are not sure about the legal requirements for collecting Personal Information, please make sure to consult with the legal/compliance department.

COLLECTING THE PERSONAL INFORMATION OF CHILDREN

Compared to adults, children's ability to judge and evaluate information is not yet mature. Therefore, children may agree to the collection, use, and provision of their own Personal Information without full understanding, and this may lead to reckless processing of their Personal Information. Because of this, special protection is necessary when processing the Personal Information of children.

Most countries often require stronger legal requirements when collecting the Personal Information of children such as also requiring the consent of a legal representative. Because the standards for children's age and the legal requirements for collecting the Personal Information of children may differ according to the regulations of each country, please make sure to check the regulations of the relevant country when processing the Personal Information of children. If you are not sure about such things, please seek help from the legal/compliance department.

5. PERSONAL INFORMATION PROCESSING AND UTILIZATION

UTILIZATION PURPOSE OF PERSONAL INFORMATION LIMITATIONS

In principle, all CJ members must only use the collected Personal Information within the scope of its utilization purpose notified at the time of its collection, and it must not be used for purposes beyond such scope.

PROVIDING PERSONAL INFORMATION TO A THIRD PARTY

If CJ members wish to provide Personal Information collected from a Data Subject to a third party for business purposes, CJ members must check in advance whether or not there is a legal basis for providing the Personal Information to the third party and the process of how to legally provide that information.

In particular, some countries may legally require prior consent from the Data Subject to provide the

Personal Information to a third party, so please keep that in mind. Because the regulations on how to legally provide Personal Information to a third party may differ by country or local jurisdiction, if you are not sure, seek help from the legal/compliance department.

Outsourcing Personal Information Processing

If we are to outsource Personal Information Processing to a third party, we must select a third party that can implement appropriate technical and managerial protection measures at the standards required by CJ. Also, when signing a Personal Information Processing outsourcing contract, we must clarify the purpose and scope of the outsourced work and clearly state the responsibilities in order to process the Personal Information safely and legally within the defined purpose of business.

Destruction of Personal Information

When the purpose of collecting the Personal Information is achieved or the retention period is over, or if the Data Subject withdraws consent or requests deletion of their Personal Information, the relevant Personal Information must be destroyed unless there is a justifiable ground permitted by applicable law or regulation. All Personal Information subject to destruction includes electronic documents, image files, and paper documents stored in computers, tablets, or folders outside of the database stored and managed through the business system.

When destroying Personal Information, take all necessary measure to prevent its recovery or regeneration. For paper documents, they must be shredded with a shredder or incinerated. For electronic documents, they must be deleted in a permanent method so they cannot be recovered.

6. Guaranteeing Transparency in Personal Information Processing

Establishing and Disclosing a Personal Information Processing Policy

Data Subjects have the right to know how CJ is processing their Personal Information. We must establish and disclose our Personal Information Processing policy that includes the Personal Information collection and processing status so that the Data Subjects can see how CJ is processing their Personal Information.

The items that must be disclosed through the Personal Information Processing policy shall be in accordance with the requirements under the regulations of each country. The Personal Information Processing policy must be easily accessible so that the Data Subjects can check it at any time, and if there is a change in content, it must be updated immediately.

7. CONFIDENTIALITY AND SAFE MANAGEMENT OF PERSONAL INFORMATION

We must take managerial and technical measures to protect Personal Information, and Personal Information must be treated valuably and processed safely according to this Policy and the regulations of each country. CJ members that process Personal Information are responsible for maintaining confidentiality, and such obligations remain in effect even after the end of employment.

MANAGERIAL PROTECTION MEASURES

CJ must appoint a person in charge of managing the Personal Information to perform the tasks related to the protection of Personal Information. The person in charge of managing Personal Information must reflect on the requirements of this Policy and the regulations of each country to establish the guidelines that will become the standard for Personal Information Processing, and CJ members must be continuously trained to understand and follow such guidelines. Also, the person in charge must periodically check to make sure that the guidelines are being followed faithfully and improve them if necessary.

The person in charge of managing the protection Personal Information must be designated according to the regulations of different countries, and because the qualifications and roles of the person in charge are specified in detail in the regulations of some countries, check the regulations to make sure CJ comply.

TECHNICAL PROTECTION MEASURES

To protect the Personal Information from the risks such as infringement, divulgence, misuse, abuse, CJ must establish and implement technical protection measures. When adopting a new service or system for processing Personal Information, the system must be designed to protect Personal Information from its planning stage, and its safety must be ensured through security reviews and improvement measures before the start of service. Such security reviews and improvement activities must not only be performed when the method of Personal Information Processing through system is changed, but also periodically even when there are no changes.

8. CROSS-BORDER TRANSFER OF PERSONAL INFORMATION

To transfer the Personal Information collected from Data Subjects across borders, CJ must ensure that the Personal Information will be safely processed and protected, and the Personal Information must be transferred only in cases where the protection measures equal to those required by this Policy

are maintained.

To transfer Personal Information across borders in accordance with the regulations of each country, some countries may require the prior consent of the Data Subject or a guarantee of the safety of the transferred information. Therefore, please check and comply with the regulations of each country.

9. Response to a Personal Information Breach

A Personal Information breach refers to breaches of security such as the destruction, loss, alteration, or unauthorized disclosure or access to Personal Information.

All CJ members must immediately notify the company if a Personal Information breach occurs, and the CJ members must identify the scope and cause of the accident as quickly as possible and take measures to minimize the damage to the Data Subject. Also, if necessary and according to relevant regulations, CJ members must immediately report the breach to the competent authorities or the country and notify the Data Subject.

To comply with this Policy, we must conduct continuous training and monitoring and periodical evaluation, and prepare crisis response plan.

10. Consequence of Violation

Any breach of this Policy is considered a violation of the Code of Business Conduct and employment contract to CJ members and a breach of contract to the third party, and it may result in disciplinary actions or the termination of business relations. Also, if any breach of Personal Information protection regulations occurs, not only CJ but also the offending CJ member may be responsible for civil, criminal, or administrative consequences of the breach, CJ members shall comply with the relevant regulations and this Policy.