CITY EXPRESS MONEY TRANSFER PRIVATE LIMITED

Privacy Policy 2019

CITY EXPRESS MONEY TRANSFER PVT. LTD.
Privacy Policy 2019

General Provisions

Article 1

The purpose of these Regulations is to ensure the appropriateness of information management and protect the rights and interests of users by stipulating matters necessary for management of information about the users of the City Express's money transfer service.

Article 2 : Definitions

The following terms used in these Regulations shall have the following meanings defined in each item below.

1. "User Information" shall mean information about the users of the City Express's money transfer service and website users, including not only information about the facts such as name, gender, date of birth, address, age, occupation, but also information representing judgment and evaluation on attributes such as body, property and occupation as well as transaction history of our money transfer service and balance account information of an individual person or its agent.
2. "Personal Information" shall mean information about existing individual persons out of User Information that can identify a certain individual by name, date of birth or other description, etc., contained in such information (including information that can easily be checked with other information and identify a certain individual by such information).
3. "User Information Controller" shall mean the Manager/Head of Legal department who specifies the parameter to disclose the information.
4. "User Information Manager" shall mean the Manager/Head of Compliance department responsible to collect, store, manage and disburse the information as required.
5. "Principal" shall mean a certain individual who can be identified by Personal Information.
6. 'User Information Officers', shall mean the 'Officers' appointed by User Information Manager from every department who shall be given required training about the management, storage and disclosure of information by Compliance Department.
7. Unless otherwise specified, any terms other than the terms listed above shall follow the definitions provided by the Act on the Individual Privacy Act 2018.

Article 3: Department Responsible for User Information Management, etc.

1. The department responsible for User Information management shall be Compliance Department. The Executive Manager/ Head of the Legal Department shall be the overall controller of User Information management (hereinafter called the "Information Overall Controller").
2. The controller of audit on the management of User Information (hereinafter called "Audit Controller") shall be the Head of Compliance Department.

Article 4 : Acquisition and Input of User Information

User Information shall be acquired in an appropriate and fair manner to the extent required for accomplishing the intended use of the information by limiting such intended use as practical as possible.

4.1 Notification and Publication of Intended Use in Acquiring Personal Information

a. If Personal Information out of User Information is acquired, its intended use shall be immediately notified to the Principal/Agent or published, except the case where such intended use is published in advance.
b. Notwithstanding the above provision, if Personal Information contained in a contract or any other document is acquired in connection with execution of such a contract with the Principal, its intended use shall be clearly notified to the Principal in advance.
c. If the intended use is changed, such changed intended use shall be notified to the Principal or published.
d. The provisions set forth in the above three clauses shall not apply to any of the following cases:

i. if the notification to the Principal or publication of the intended use may do harm to the rights or fair profits of the Company;
ii. in the case where it is required to assist any government agency or local government in performing its due process required by law, if the notification to the Principal or publication of the intended use may interfere with the performance of such due process of law;

Article 5: Person in Charge of Acquisition and Input of User Information, etc.

i. The Information Manager shall appoint a person in charge of acquisition and input of User Information depending on business needs from the concerned department as 'Privacy Champions' and any persons other than the person in charge shall not acquire or input User Information.
ii. The Information Overall Controller shall set a limit on information to be acquired and input depending on business needs, and the person in charge of acquisition and input of User Information shall not acquire or input any information other than such information.
iii. If the person in charge of acquisition and input of User Information performs any work other than the work specified by the Information Overall Controller, the person in charge shall notify the Information Overall Controller of such work in advance for approval.

Article 6: Confirmation Procedures of Information Related to Use and Processing

i. The Information Manager shall formulate procedures to check and confirm the number and content, etc., of User Information used and processed, and shall cause the person in charge to implement the procedures.
ii. The Information Manager shall review the records checked and confirmed in accordance with the above procedures, and shall store such records in a specified place for a specified period of time, as necessary.
iii. The Information Manager shall check such records as stored in accordance with the above clause regularly.

Article 7: Taking-Out of User Information Outside the Controlled Area at a Stage of Use and Processing

If User Information is taken out from the specified storage place at a stage of use and processing of information, the person in charge of use and processing of the information shall obtain the approval of the Information Overall Controller by submitting a written request indicating the following items:

1. Name of the person in charge related to taking-out
2. Details of User Information intended for taking-out
3. Purpose of taking-out
4. Devices or media that contain a record of the information to be taken out
5. Period during which the information is taken out

Article 8: Disclosure of Information

8.1. Subject to the consent or as otherwise permitted by law, the delegated information provider/company may disclose the Information collected in the paragraphs titled, "INFORMATION" and "COOKIES & INTERNET TECHNOLOGY" to our Affiliates and to unaffiliated third parties as described below for any of the purposes described in the statement, including those described in the paragraph entitled “USE OF INFORMATION”.

8.2 The disclosure of Information with the following CITY EXPRESS Affiliates to effect, administer and complete transactions or deliver products or services including, but not limited to:

1. CITY EXPRESS group companies.
2. Companies helping to run or improve the running of the business or help in delivering services to the customer and to banks.
3. In order to comply with legal, regulatory, security and processing requirements, government and foreign government requirements, applicable to the company or its Affiliates or service providers, including but not limited to anti-money laundering laws; and
4. To organizations which help to process transactions, validate customer information, and helps us prevent debt, fraud, theft or loss;

5. As permitted or required by law.

The disclosure of Information about current and former customers to perform marketing, business analysis and advertising services to companies having contractual or joint marketing arrangements upon notice of unambiguous consent (opt-in) for the use of Information for these purposes.

Article 9: Disposal of Data

If any paper or magnetic media, etc., that contain User Information are erased or disposed of, it shall be carried out in an appropriate manner by means of shredding, incineration, melting, magnetic erasure or destruction in accordance with the instructions of the Information Manager depending on the content of the relevant information. If erasure or disposal work is assigned to any party other than the Company, a certificate of erasure or disposal shall be obtained, and the fact of erasure or disposal shall be checked as necessary.

Article 10: Prohibition of Acquisition, etc., of Sensitive Information

Any Personal Information that contains any of the following items shall not be acquired, used or provided:

1. Matters concerning thought, belief and religion
2. Race, ethnicity, place of origin, registered domicile (excluding information about present address), physical and mental disability, criminal history and any other matters that cause social discrimination
3. Matters concerning the right to organize, bargain collectively and any other work in groups of working persons
4. Matters concerning participation in demonstration and exercise of the right of petition and any other political rights
5. Matters concerning health and medical care.

Article 11: Restriction on Provision to Third Party

1. Unless otherwise specified by law and these Regulations, User Information including Personal Information shall not be provided to any third party.
2. If any employee who handles User Information deems it necessary to provide User Information to any third party, such an employee shall give notice to the Information Overall Controller for approval, whether it contains Personal Information or not.
3. Unless otherwise permitted by law, if Personal Information is included in the information to be provided with respect to such notice as set forth in the previous clause, the Information Overall Controller shall give approval after obtaining the informed consent from the Principal on the following items:

1. Name of a third party to which User Information is provided
2. Intended use by the third party who receives User Information
3. Content of the information to be provided to the third party

Article 12: Management and Supervision of Employees, etc.

1. For employees' handling of User Information, the department responsible for User Information management (Compliance Department) shall set up an appropriate internal management system by appointing Human Resource Manager as 'Privacy Officer' to ensure safety management of the information, and shall exercise necessary and appropriate supervision over the employees.
2. "Necessary and appropriate supervision" as set forth in the previous clause shall be exercised by the following system, etc.:

1. to enter into an agreement, etc., with employees at the time of recruitment, etc., which obliges the employees not to disclose User Information obtained in connection with the City Express's business, etc., to any third party or use it for any purposes other than the intended purpose while in office and after retirement;
2. to define the role and responsibility of employees, familiarize officers and employees with, and provide education and training to officers and employees concerning their duties of safety management through development of regulations for appropriate handling of User Information;
3. to maintain a system to check the compliance status, etc., on the matters specified in the internal safety management measures and conduct inspection and audit on the protection of User Information by employees in order to prevent taking-out of User Information by employees.

Article 13: Investigation

The Information Overall Controller shall conduct an investigation on the following items to check the fact situation:

1. Actions to preserve evidence
2. Confirmation of the fact of the leak, etc.
3. Identification of User Information involved in the leak, etc. (object person, attributes, number of items, etc.)
4. Investigation of the route and cause of the leak, etc.

Article 14 : Prevention of Expansion of Damage

In the event of a leak accident, etc., the Information Overall Controller shall make efforts to prevent damage from expanding by implementing the following measures, etc.:

1. Collection of leaked information, etc.
2. Development and implementation of preventive measures for a case where highly useful information such as card number, password, account number is leaked and there is a high risk of secondary damage, etc.

Article 15: Outsourcing of Handling of User Information

1. If all or any of handling of User Information is outsourced to any third party, the person in charge of handling such User Information shall give prior written notice to the Information Overall Controller for approval.
2. The Information Manager shall take the following measures, and shall make an application to the department responsible for User Information management for approval of the Information Overall Controller before entering into a contract with a subcontractor:

1. to conduct an interview with a responsible person of the subcontractor and conduct on-site review at the information processing facility of the subcontractor to ensure that the level of protection and security management of User Information is the same or higher than the Company;
2. to obtain financial information about the subcontractor to ensure its financial safety;
3. to set forth necessary provisions in a consignment contract in accordance with the Act on Settlement of Funds, Act on the Protection of Personal Information and any other applicable laws and regulations as well as the policies and guidelines, etc., of the authorities concerned, and also set out necessary provisions concerning confidentiality and safety operation, etc., in such a consignment contract to ensure safety.

3. During the term of the consignment contract, the person in charge shall check whether the subcontractor complies with the contract with the Company. In the event that any violation of the contract is found, the person in charge shall give notice to the Information Overall Controller to that effect.
4. The Information Overall Controller shall keep documents including a consignment contract, audit reports and notice letters, etc., prepared under this Article (including electromagnetic records) for Five (5) years after the termination of the contract.

Article 16: Disclosure of Information

1. If the department responsible for User Information management is requested to make disclosure of Personal Information (limited to information related to the Principal. This phrase shall apply by the Principal, it shall disclose Personal Information to the Principal without delay in accordance with the method permitted by the Principal, except the following cases:

i. if it may do harm to the life, body, property and any other rights and interests of the Principal or any third party;
ii. if it may significantly interfere with the fair practice of business of the Company;
iii. if it may result in the violation of the applicable laws.

2. If the department responsible for User Information management cannot disclose Personal Information, it shall give notice to the Principal without delay and explain the reason by indicating grounds for such decision and the facts constituting the grounds.

Article 17 : Correction

1. If the department responsible for User Information management is requested to correct, add or delete any Personal Information by the Principal on grounds that it is not true (hereinafter called "Correction, etc."), it shall conduct a necessary investigation, including confirmation of facts, without delay, and shall make a Correction, etc., of such Personal Information based on the results.
2. If the department responsible for User Information management makes a Correction, etc., or decides not to make a Correction, etc., of any Personal Information requested by the Principal, it shall give notice to the Principal to that effect without delay (including grounds for the decision and the facts constituting the grounds not to make a Correction, etc., if it makes such a decision).

Article 18: Procedures of Complying with Request for Disclosure

1. The department responsible for User Information management shall set out the following items with respect to the request for disclosure as set forth in Article 16:

1. An application to be submitted in requesting disclosure;
2. Method of identification of a person who requests disclosure;
3. Method of answer to the request for disclosure, etc.