Policy on Handling of Personal Information in Fund Transfer Services

General Provisions

DIGITAL WALLET Corporation and its group companies ("the Group") position the protection of personal information of customers as one of the most important management priorities when providing fund transfer services ("Fund Transfer Services"). This "Policy on Handling of Personal Information in Fund Transfer Services" ("this Handling Policy") stipulates the Group's policy for collecting, using, and managing customers' personal information through Fund Transfer Services offered via applications etc.

In this Handling Policy, "Personal Information" refers to "personal information" as defined under the Act on the Protection of Personal Information, including "personal identification codes" and "sensitive personal information" for which extra care is required to prevent prejudice or disadvantage. "Personal Information Protection Commission" means the government agency established as an external bureau of the Cabinet Office in 2016.

The Group complies with the amended Act on the Protection of Personal Information fully implemented in April 2022 and all related laws, regulations, and guidelines, and appropriately handles customers' personal information.

Article 1 (Acquisition of Personal Information)

The Group acquires personal information from customers by lawful and fair means and does not use false or other improper methods. The Group prohibits the improper use of personal information. The Group may acquire personal information by the following means:

1. Information directly provided by the customer when registering or using an account for Fund Transfer Services
2. Information automatically collected during the use of Fund Transfer Services
3. Information provided by business partners with the customer's consent
4. Information acquired lawfully from public sources

Article 2 (Types of Acquired Personal Information)

The types of personal and related information acquired by the Group are as follows:

(1) Information provided by the customer

- Name, date of birth, gender, email address for Fund Transfer Services, phone number, address
- Images and biometric data (e.g. facial photographs)
- Information necessary for identity verification (nationality, residence status, period of stay, declaration regarding foreign PEP status, etc.)
- My Number and My Number Card information (when acquired pursuant to laws)
- Information on the customer's and recipient's bank accounts, etc.
- Login authentication information for Fund Transfer Services
- Contents of inquiries to the Group
- Information related to responses and verification requests from the Group
- For recipients (or beneficial owners if the recipient is an entity): name, date of birth, gender, address, contact information, nationality, relation to customer
- Official documents proving the above personal information

(2) Automatically collected information

- Device information (type, OS, IP address, etc.)
- Access log information (date/time, page views, etc.)
- App/service usage history (transaction records, payment history, etc.)
- User ID and authentication information assigned by the Group
- Location information (if authorized by the customer)
- Cookie and local storage information (if authorized by the customer)

- Payment information (if using domestic payment services)
- Other information collected in connection with remittance or payment services

(3) Information provided by third parties

- Personal information and related data of customers, employees, business partners, and related persons
- Social media login information
- Attribute data from advertising operators

Article 3 (Purposes of Use of Personal Information)

The Group handles customers' personal information within the scope necessary to achieve the following purposes and does not use such information for purposes other than these. Measures are taken to prevent use for unintended purposes.

(1) Provision of services related to fund transfer business

- Opening accounts, executing transactions, instructing banks or contractors to remit monies
- Identity verification, checking, and recording transaction details, recordkeeping
- Calculating, billing, and settling service usage fees
- Ensuring transaction security, detecting, and preventing unauthorized use

(2) Improvement and development of new services

- Enhancing service quality, devising new features/services
- Analyzing service usage (statistically aggregated so a specific individual cannot be identified)

(3) Communication with customers

- Sending important notices regarding services
- Responding to inquiries and support requests
- Conducting surveys

(4) Marketing activities

- Advertising or promoting the Group's services
- Providing personalized information tailored to customer needs
- Notifying about campaigns and promotions

(5) Compliance with laws and protection of rights

- Fulfilling legal obligations (e.g., checking against sanction lists, identity verification, recordkeeping, etc.)
- Reporting to financial authorities, responding to inquiries based on laws
- Protecting the rights of the Group and third parties

Article 4 (Security Management of Personal Information)

To prevent leakage, loss, or damage ("incidents") of personal information, the Group implements the following security management measures:

(1) Organizational Safety Management Measures

- Appointment of a Personal Information Protection Manager
- Establishment of internal rules related to personal information protection
- Education and training of employees
- Regular audits on the status of personal information handling

(2) Human Safety Management Measures

- Execution of confidentiality agreements with employees
- Management and periodic review of access permissions

(3) Physical Safety Management Measures

- Access control for areas handling personal information
- Physical measures to prevent theft and loss

(4) Technical Safety Management Measures

- Access control, implementation of authentication systems
- Encryption of communications
- Countermeasures against unauthorized access
- Recording and analysis of operation logs
- Use of major cloud service providers' servers located in Japan

Article 5 (Data Controller and Data Protection Contact)

The Data Controller and Data Protection Contact handling customer personal information are as follows:

Digital Wallet Corporation, Systems Division: Data Protection Manager

Kioi-cho, 3-6, Chiyoda-ku, Tokyo, 102-0094

E-mail: info@digitalwallet.co.jp

For questions, requests, complaints regarding application of this Handling Policy, or to exercise rights for disclosure, correction, and deletion of personal information held by the Group, please send a written request or email to the above address.

Article 6 (Retention Period of Personal Information)

The Group retains personal information for the following periods:

(1) Where laws prescribe a retention period, for the legally required period:

- Fund transfer transaction records: 10 years after transaction completion
- Identity verification records: 7 years after transaction completion
- Personal information obtained from third parties: 3 years after receipt

(2) Where laws do not prescribe the period, for the period necessary to fulfill purposes:

- Until claims or debts expire after contract termination
- For as long as necessary to respond to contracts and inquiries
- For other reasonable periods necessary to achieve legitimate business objectives

Article 7 (Provision of Personal Information to Third Parties)

Except in cases described below, personal information will be provided to third parties in accordance with this Handling Policy upon the customer's agreement.

1. Where required by law
2. When necessary for the protection of life, body, or property
3. When especially necessary to promote public health or sound nurturing of children
4. When cooperating with administrative authorities or agents to perform duties prescribed by law
5. When necessary to provide academic research institutions (where personal data is used for research, except where it would unjustly harm the interests of the individual)

(1) Joint Use within the Group

- Scope and users: DIGITAL WALLET Corporation, Digital Wallet Solutions, and group companies under its parent company's umbrella
- Personal Information jointly used: Information provided by customers (see Article 3.1), information automatically collected (Article 3.2)

- Purpose: Within the scope of Article 4
- Managing entity: DIGITAL WALLET Corporation

(2) Provision to Contractors

- Handled within the necessary scope for achieving the purposes specified in Article 4
- Contractors are obligated to manage personal information appropriately and are supervised

(3) Provision to Third Parties located abroad

- Provided only to officially authorized financial institutions, countries/regions recognized for adequate protection systems, or organizations maintaining measures equivalent to those required of data handlers in Japan
- Information on foreign contractors disclosed via the register of fund transfer businesses (refer to Ministry of Finance Kanto Finance Bureau)

(4) Provision to Third-Party Service Providers

- Examples: Foreign exchange, remittance, payment, cloud services, customer support, data analysis, marketing, card mailing
- Access only for providing relevant functions, no use beyond that scope

(5) Legal Protection and Law Enforcement

- Disclosure may be made if necessary for legal compliance or to protect the rights, property, or safety of the Group/customers

Article 8 (Handling of Pseudonymized and Anonymized Information)

The Group may process personal information into pseudonymized or anonymized information.

(1) Pseudonymized Information

- Created as stipulated by law so specific individuals cannot be identified, used for analyzing service trends, statistics for new service development, marketing analysis
- Pseudonymized information is processed according to legal standards with security to prevent re-identification and will not be provided to third parties

(2) Anonymized Information

- Created by processing personal information so it cannot be used to identify individuals, may be used for market research, statistical analysis, academic research, collaboration with business partners
- Processing and provision follow legal standards, and use by recipients is appropriately supervised

Article 9 (Rights to Disclosure, Correction, Deletion, etc.)

(1) Customers have the following rights:

1. Disclosure Rights

- Contents of personal information held
- Purpose of use
- Record of provision to third parties

2. Correction/Addition/Deletion Rights

- For correcting, adding, or deleting inaccurate content

3. Usage Suspension/Deletion Rights

- For illegal or improper acquisition/use, excess usage, provision to third parties without consent

4. Suspension of Third-Party Provision Rights

- For provision to third parties without consent

(2) International Regulations

- The Group responds according to jurisdictional law (e.g., GDPR, PIPEDA, PIPL) applicable based on customer residence or service use location

(3) Request Handling

- Requests are responded to as required by law, except in cases such as mandatory retention, failure to verify identity, requests falling under legally recognized exceptions, major business impediments, potential harm to third-party rights/interests, clearly unreasonable or excessive (including repeated) requests
- Requests can be made from the fund transfer service app [Help Center]

(4) Obligations of Customers

- Customers are obligated to ensure that information provided to the Company is accurate and up-to-date and to promptly notify or update information if there are changes.
- If concerns related to leakage or misuse of customer information are recognized, customers must promptly contact the Company.
- The Company shall not be liable for damages caused or derived from failure to fulfill these responsibilities.

Article 10 (Response to Incidents such as Data Leakages)

In the event of, or potential for, incidents affecting personal information, the Group will:

1. Report to management, prevent further harm
2. Investigate and clarify facts, determine cause

3. Identify the scope of impact
4. Consider and implement recurrence prevention measures
5. Notify affected customers
6. Report to supervisory authorities (Financial Services Agency)
7. Disclose it on the Group's website if necessary

Immediate Reporting Required

- For incidents affecting sensitive personal information, potential financial damage, suspicion of improper acts, cases involving leakage of personal data of over 1,000 individuals, leakage of identification codes

Article 11 (Use of Cookies)

The Group uses cookies and similar technologies to enhance customers' application experiences.

(1) What are cookies

Cookies are small text files that websites store on your device. While cookies do not directly contain personal information, they include data that can identify your browser or device.

(2) Types and purposes of cookies used

Essential cookies: Needed for the basic operation of fund transfer services

Functional cookies: Remember user settings and provide customized experiences

Analytics cookies: Analyze usage in order to improve services

Marketing cookies: Show ads tailored to user interests

(3) Cookie management

Users can limit acceptance of cookies or receive notifications when cookies are set by adjusting browser settings. Refusal of essential cookies may result in some fund transfer service features not working properly.

Article 12 (Use of Google Analytics)

The Group uses Google Analytics to understand website usage.

Google Analytics uses cookies issued by the Group so Google Inc. can collect, record, and analyze access history. The Group receives aggregated results without identifying individuals.

For details on Google's data collection and processing, see:

- How Google uses data when you use partner sites or apps:

  https://policies.google.com/technologies/partner-sites?hl=ja

- Google Analytics opt-out browser add-on:

  https://tools.google.com/dlpage/gaoptout?hl=ja

- Google Analytics Terms:

  https://marketingplatform.google.com/about/analytics/terms/jp/

- Google Privacy Policy:

  https://policies.google.com/privacy?hl=ja

Article 13 (International Data Transfers)

The Group's business may require international data transfers. For cross-border transfers of personal information, the Group takes appropriate protections including:

- Compliance with local personal information protection laws
- Appropriate contracts with foreign contractors
- Risk assessments and periodic audits or standardized Wolfsberg questionnaires

Applicable requirements include GDPR (EU General Data Protection Regulation), PIPEDA (Canada Personal Information Protection and Electronic Documents Act), PIPL (China Personal Information Protection Law), etc., as appropriate for each location.

Article 14 (Changes to This Handling Policy)

The Group may change this policy due to amendments to law, business content changes, or advances in security technologies.

If there are significant changes, customers will be notified promptly by website posting, email, or app notifications.

Revised policies take effect when posted to the Group's fund transfer service website. The latest version is always available on the website under "Privacy Policy."

Last modified: October 8, 2025

Digital Wallet Corporation