

DEX INTERNATIONAL LIMITED

PRIVACY POLICY

DECEMBER 2023

Version 1.0



Contents

Page 2	Amendments
Page 2	Introduction
Page 3	Distribution List
Page 3	Document Owner
Page 3	Legal and Regulatory Requirements
Page 4	How to contact DEX about Privacy and Data Protection
Page 4	Types of Personal Data and how it is obtained
Page 5	Legal basis for using Personal Data
Page 6	How DEX processes Personal Data
Page 7	How DEX shares Personal Data
Page 7	International Personal Data Transfers
Page 8	Marketing Preferences
Page 8	Data Retention, Data Security and Data Protection
Page 9	Customer Rights

Amendments

VERSION NUMBER	DRAFTED BY	DATE
1.0	John Tomlinson	17/12/2023

Introduction

This policy and procedure document sets out the principles and processes DEX International Limited (“DEX”) follows in order to collect, store, use, share and process customers’ personal data whenever the customers use the firm’s website, services, or mobile applications (the “App”).

It also details the rights customers have in respect of DEX’s use of their personal data.

Personal data means any information about an identified or identifiable individual. It does not include anonymous data which cannot be linked back to an individual, and it is not relevant whether any personal data is in the public domain.

DEX is an Authorised Payment Institution in the United Kingdom that is authorised and regulated by the Financial Conduct Authority (FCA Firm Reference Number: 503929) and registered with His Majesty’s Revenue and Customs (MLR number: XMLL00000116021).

DEX possesses the following FCA regulatory permissions: MONEY REMITTANCE

DEX offers international remittance services via several options including its App and is responsible for processing customers’ personal data.

Distribution List

NAME	LOCATION
Adeel Salman	High Wycombe, UK
Muhammad Rashid Haroon	High Wycombe, UK
John Tomlinson	High Wycombe, UK
Alamgir Malik	Pakistan global headquarters

Document Owner

The original template was drafted by John Tomlinson, Head of Compliance of DEX International Limited – compliance.uk@dex-intl.com

Legal and Regulatory Requirements

Within the United Kingdom the Information Commissioner’s Office (“ICO”) is the data protection authority tasked with safeguarding the interests of the users of DEX’s services: <https://ico.org.uk/>

DEX Privacy Policy primarily adheres to UK legal and regulatory obligations. The data protection legislation applicable to DEX and associated entities includes, but is not limited to, the UK General Data Protection Regulations, EU General Data Protection Regulation, UK Privacy Electronic Communications Regulation 2011, and the EU e-Privacy legislation.

However, this is a global Privacy Policy which means that the personal data protections apply to all customers and their personal data regardless of their location.

How to contact DEX about privacy and data protection

United Kingdom Customers can contact the firm about their privacy and personal data, to exercise their data rights and for information about how DEX uses, processes, stores, and protects personal data by emailing us at privacy@dex-intl.com

Our Data Protection Officer (“DPO”) is John Tomlinson, who can be contacted via the above email address.

Types of personal data and how it is obtained

DEX mainly processes personal data provided directly to the firm by its customers. However, DEX may also process personal data of individuals other than customers, such as recipients of payments and other making enquiries or complaints. The table below sets out the information collected and processed and where it is obtained. The collection and use of personal data is essential in order to provide remittance payment services in a secure manner, guaranteeing accurate, rapid payments and minimising the risks of fraud, money laundering, and other criminal activity.

<p>Information collected when you:</p> <ul style="list-style-type: none"> - register for the App; - use our Services; - fill your details and transaction details; - correspond with us; - respond to any of our Services; - take part in online discussions; - speak with a member of our team - enter competitions; and/or - contact us for other reasons. 	<ul style="list-style-type: none"> - Name, address and date and place of birth - E-mail address, phone number and details of the device you use (e.g. device ID). - Income and occupation. - Proof of address. - Details and copies of your identification documents (for example passport or government ID) and your image to compare against these (either in photo or video form). - Records of our discussions, if you contact us or we contact you (including records of phone calls and chat conversations). - Your geographical location and IP address. - Your device settings (e.g. language preference, time zone). - Information relating to your transaction (e.g. the person you are sending money to, payment reason). - Information relating to how you pay us (e.g. encrypted card information and bank details) - Credit reports and other consumer report information.
<p>Information collected when you use our Services on our App or website</p>	<ul style="list-style-type: none"> - Information on use of DEX products, including the date, time and amount of transfers, currencies and exchange rate used, beneficiary details, your IP address, messages sent or received, details of device used to make payment and the payment method used. - Technical information, including your IP address, login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform. - Information about your visit, including the full URL clickstream to, through and from our Website or App (including date and time); page response times, download errors, length of visits to certain pages, page interaction information, methods used to browse away from the page. - Optional information: <ul style="list-style-type: none"> - If you turn on location services on or in the App, we receive information about your location using GPS technology. - If you give us access, information stored on your device like contact information from your contacts list.

Information DEX collects from others.	Information from your use of third-party applications, such as the Apple App Store or Google Play Store, social networking sites, such as name, your social network ID, location information, email, device ID, browser ID, and profile picture. Your use of third-party applications is subject to the privacy policy and terms of service for such applications. Information from our service providers in destination countries, such as names associated with particular phone numbers.
Information DEX collects from social media.	Occasionally, DEX uses publicly available information about you from selected social media websites or apps to carry out enhanced due diligence checks (to comply with our anti-money laundering or sanctions screening obligations).
Information gathered from other public sources.	DEX has a legal obligation to verify your identity as part of our anti-money laundering checks. To do this we collect information and contact details from publicly available sources, such as online registers or directories.

In limited circumstances, DEX collects, processes and stores sensitive personal data in order to comply with legal and regulation obligations – e.g. biometric data to undertake anti-money laundering checks or to prevent fraud. All such sensitive personal data is subject to appropriately robust protections.

Legal basis for using Personal Data

At all times DEX must have a valid legal justification for using personal data.

The legal bases for use of customers’ personal data are:

- **Contractual obligations:** It is impossible to provide remittance services securely and safely without using personal data. At the outset, personal data is required in order to enter into agreements with customers, and, thereafter, to meet the firm’s contractual obligations. Whenever personal data of a special, sensitive nature is processed (i.e. biometric data or data which may reveal political opinions) is used, it is processed on the additional legal basis that such processing is necessary for substantial public interest reason – e.g. to prevent or detect unlawful activity.
- **Legal Obligations:** It is often the case that DEX has a legal responsibility to collect and store personal data – for example to comply with anti-money laundering legislation DEX must collect and retain certain information about its customers.
- **Legitimate Interests:** Where it is necessary for DEX’s legitimate interests, or those of a third party, and customers’ interests and fundamental rights do not override such interests.
- **Consent:** DEX customers can provide explicit consent to process their personal data to facilitate the provision of payment services.

How DEX uses Personal Data

DEX uses personal data for the reasons listed below.

To provide payment services:

- To fulfil agreements with customers and otherwise administer the customer relationship.
- To process payments and prove transactions have been executed.
- To process information about customers' contacts to make it easy for them to find and connect them and improve payment accuracy.
- To administer profiles of users on our databases.
- To provide customer support (we may record and monitor any communications, including phone calls, to maintain appropriate records, check instructions, or to analyse, assess and improve our services for quality and training purposes).
- To provide, maintain, personalise, optimise, and improve the services, including research and analytics regarding use of the Services, or to remember customers who leave and later return to use our services.

To keep our Services up and running:

- To monitor website and App usage, including to determine enhancements and technical improvements.
- For customer analysis, to administer our services, and for internal operations - for example troubleshooting, data analysis, testing, research, and statistical purposes.

To meet our legal obligations and enforce our rights:

- To confirm customers' identity and verify their personal and contact details.
- To comply with applicable laws, including anti-money laundering, counter terrorist financing and sanctions laws, including to verify customer identity.
- To establish, exercise or defend a legal claim.
- To action any data subject right requests.
- To meet our legal and regulatory obligations.

To protect you and other users against fraud:

- To detect, investigate and prevent activities which may be fraudulent or illegal, or which may misuse our services or break our policies.
- To comply with financial crime laws and to confirm that a customer is eligible to use our services. We also use it to help us manage fraud risks related to your account.

To communicate with customers:

- To communicate with customers in relation to our services, including to notify them of changes, seek their views or comments on our services, and to handle any enquiry or complaints.

For marketing and providing other services that might benefit customers:

- To improve our services and for general business development, for example to develop new products and features and explore new business opportunities.
- For marketing, product and customer analysis, including testing, for example to improve our product range and to optimise our customer offerings.
- To be able to administer customer participation in competitions, promotions and events.
- To provide customers with information, news, and marketing about our services, including where we partner with others to offer similar services.

How DEX shares Personal Data

Due to the nature of DEX's business, there may be times we share personal data with the following third parties. Note that DEX does not ever sell personal data.

- **DEX service providers:** We will share personal data with DEX group companies and with partners who provide us with services that we need in order to provide our services to customers, for example:
 - Suppliers who provide us with IT, payment and delivery services;
 - Suppliers who help us meet our legal and regulatory obligations, such as identity verification service providers and background check providers (these providers may use your data to conduct checks with credit reference agencies, financial or credit institutions, official registers and databases, as well as fraud prevention agencies to verify your identity);
 - Our banking and financial services partners and payments networks;
 - Analytics providers and search information providers;
 - Customer-service providers, survey providers and developers and
 - Communications service providers.
- **For legal reasons:** There may also be instances where DEX needs to share data with a competent law enforcement body, regulatory body, government agency, court, or other third party where DEX reasonably believes disclosure is necessary (i) as a matter of applicable law or regulation or (ii) to exercise, establish or defend the firm's legal rights.
- **To advertisers and advertising networks, analytics, and search engine providers:** DEX provides limited information about customers' in-App activity (not personal data) with these providers solely to select and serve relevant adverts to our customers and others.

International Personal Data transfers

DEX offers international remittance payment services, and therefore needs to transfer customers' personal data across borders.

Personal data may be transferred to, and stored and processed in, the European Union, the United States, or any other country in which we or our affiliates, subcontractors, vendors, or partner payment processors maintain facilities.

The laws in other countries regarding personal information may be different from the laws of the United Kingdom. Any such transfers will comply with safeguards required by relevant local law. It may also be processed by staff operating outside the country customers are located in, who work for us directly or for one of our payment processors. Such staff may be engaged in, among other things, the fulfilment of a customer's payment order, the processing of their payment details, and the provision of customer support. By submitting their personal data, our customers agree to this transfer, storing or processing.

If DEX transfer personal data to another country that doesn't offer a standard of data protection equivalent to the UK, we will make sure that personal data is sufficiently protected. For example, we make sure that a contract with strict data protection safeguards is in place before we transfer UK customers' personal data.

Marketing Communications

DEX may elect to use the contact details of customers to send them marketing communications about its services by email, telephone, SMS, WhatsApp, push notification, social media, or other communication formats. This may include news, promotional offers, opportunities to enter competitions and win prizes and updates regarding DEX and its services, including new services and products.

Customers have the right to ask DEX not to process their personal information for marketing purposes. They can exercise this opt-out right at any time by telling DEX or following the instructions in the communication e.g. unsubscribing from emails and SMS. DEX will respect this choice and will stop sending such communications as soon as reasonably practicable and at the latest within one month of receiving a request to unsubscribe. Customers are free to change their marketing choices at any time. We may contact customers to reaffirm their consent to marketing.

If customers do opt-out, we may still send them important services and administrative messages, from which they cannot opt-out.

Data Retention, Data Security and Data Protection

Data retention

DEX will generally keep personal data for ten years after our business relationship ends, or for as long as necessary in line with local requirements, such as for example, best practice recommendations (e.g. supervisory authority recommendations), relevant guidelines (e.g. employment guidance) or for as long as mandated under specific legislation (e.g. tax laws).

DEX will also determine appropriate retention periods based on our legitimate interests where identified. As a regulated financial institution, we are required by law to store some data beyond the termination of the relationship with us. After such time, personal data will only be accessed or processed if absolutely necessary. DEX always deletes data that is no longer required by relevant legislation. When personal data needs to be deleted, DEX will delete it manually or automatically, or anonymise it in the event outright deletion is not possible.

Data security

DEX has implemented appropriate security measures to prevent personal data from being accidentally lost, used, accessed in an unauthorised way, altered, or disclosed. DEX uses reasonable physical and technical safeguards to protect personal information, both during transmission and storage. No method of transmission over the internet, including by email, or method of electronic storage is 100% secure, so it is never possible to guarantee its absolute security.

All information provided to DEX is stored on secure servers. Any payment transactions will be . Customers are responsible for keeping confidential any passwords. We ask them not to share passwords with anyone else and not to use passwords for other services or products.

In addition, we limit access to personal data to those who need it to do their jobs (i.e. employees, agents, contractors and other third parties with a business need to know). If this is a third party, they will only process personal data on DEX's instructions and will be subject to a duty of confidentiality.

Data protection rights

Data protection laws enable several rights in relation to how an organisation processes customers' personal data. If a customer would like to exercise any of the below rights can do so by sending us a written request to privacy@dex-intl.com

The customer's ability to exercise these rights will depend on a number of factors. Sometimes, DEX won't be able to agree to a request (for example, if we have a legitimate reason for not doing so or the right does not apply to the particular information held). If a customer objects to DEX using personal data which is needed in order to provide services, DEX may need to close their account.

Customer Rights

UK national law provides for the following rights to customers:

- **Right to be informed** - Customers have the right to know what personal data we collect about them, how it is used, for what purpose and in accordance with which lawful basis, who DEX shares it with and how long DEX keeps it.
- **Right to access data** - Customers have the right to receive a copy of the Personal Data DEX holds about them (this is sometimes referred to as a "Subject Access Request").

- **Right to rectification** - Customers have the right to have any incomplete or inaccurate information held about them corrected. Customers can also make updates themselves within the App.
- **Right to erasure** - Customers have the right to ask DEX to delete their personal data if it is no longer necessary for the purpose for which it was collected or needed by DEX to meet its legal obligations or for a legitimate interest.
- **Right to restrict processing** - Customers can instruct DEX to stop using their personal data, including for marketing purposes.
- **Right to objection** - Customers have the right to object to DEX processing their personal data. If the firm's legal basis for using personal data is 'legitimate interests' and a customer disagrees with us using it, they can object. However, DEX will assess whether its interests are overridden by a customer's fundamental rights and freedoms.
- **Right to portability** - Customers can ask DEX to transfer personal data to them or to another company.

COMPLAINTS

Customers who have concerns or complaints in relation to DEX's Privacy Policy and in relation to how their personal data is processed may contact DEX directly by emailing privacy@dex-intl.com

If a customer is unsatisfied with DEX's response, they may contact the UK Information Commissioner's Office by emailing: <https://ico.org.uk/>