

Data Protection Policy

Mercantile EXCHANGE

House UK LTD

2023

Company Information

Company No: - 07456837

FRN:- 543098

Registered office address

108 Whitechapel Road

London E1 1JD

Contents

INTRODUCTION	4
Purpose:	4
DATA PROTECTION/GDPR:.....	5
Scope:	5
Out of Scope	5
Policy:.....	5
Principles	6
Data Collection:	7
The Right of Data Subjects	7
User Authorization and Control:	8
Users:.....	8
Systems:	8
Reporting Requirements:	8
Employee Requirements:	8
Actions:.....	9
Lawful, Fair and transparent Data Processing	9
Specified, Explicit and legitimate Purpose.....	11
Profiling	11
Personal Data Collected, Held and Processed	12
Data Security - Transferring Personal Data and Communications	12
Data Security – Storage	12
Data Security – Disposal	13
Data Security - Use of Personal Data.....	13
Data Security - IT Security	14
Record keeping:.....	14
Data Protection Impact Assessments.....	14
Data subject Access	15
Rectification of personal Data.....	15
Ensure of personal data	16
Restriction of Personal Data Processing.....	16
Data portability	17
Objections of Personal Data Processing	17
Automated Decision Making.....	17

Profiling	18
Personal Data Collected, Held and Processed	18
Keeping Data Subject Informed	18
Ownership and Responsibilities:	19
Restriction of Personal Data Processing.....	20
Data Portability	20
Transferring Personal Data to a Country Outside the UK	20
Data Breach Notification	21
Organisational Measures	22
Annual Internal Control Program:.....	23

INTRODUCTION

MERCANTILE EXCHANGE HOUSE (UK) LIMITED is the company that is incorporated on 1st of December 2010 also it is registered as Small Payment Institution on 09/08/2018. This company is providing initially money remittance to Bangladesh or closely connected to Bangladesh and will be sending to other corridors in near future.

These policies and procedures apply to all members/staff of MERCANTILE EXCHANGE HOUSE (UK) LIMITED.

This document will be provided to the CEO & MLRO of the Company – and he will have to ensure that all the members agree to abide by the policies outlined.

Purpose:

In order to avoid negatively harming consumers, incurring penalties for non-compliance, and suffering damage to our brand, MERCANTILE EXCHANGE HOUSE (UK) LIMITED must restrict access to personal and sensitive data to prevent it from being lost or compromised. At the same time, we must ensure that users have access to the data they need to do their jobs.

The policy does not guarantee that all malicious data theft will be prevented. Rather, it describes the parameters for data breach prevention with the primary goal of increasing user awareness and avoiding inadvertent loss scenarios.

The objective and benefits of this policy are to create awareness of MERCANTILE EXCHANGE HOUSE (UK) LIMITED's data protection safeguards in order to guarantee that a consistent and uniform approach is taken in the future.

- Employees are aware of their rights and obligations in connection to information handling;
- Information is gathered, processed, held, transferred, and disposed of responsibly.
- Appropriate processes have been put in place to ensure that persons about whom the Company has information are protected.

The latest regulatory provisions for data protection, including the EU General Data Protection Regulations (GDPR) and any guidance published by the UK Information Commissioner, are taken into account when developing and reviewing Company records management policies and procedures.

This policy document is intended for all MERCANTILE EXCHANGE HOUSE (UK) LIMITED employees in order to safeguard all sensitive information. This policy also applies to the company's server database and the IT system that maintains sensitive information, as well as all computers used for email, web access, or other web-related activities.

DATA PROTECTION/GDPR:

GDPR stands for General Data Protection Regulation, and it is the world's strongest privacy and security law. Despite the fact that it was designed and passed by the EU (European Union), it imposes duties on any organisation that targets or collects data about EU citizens.

GDPR went into force on May 25, 2018, and the law stipulates that anyone who breaks its privacy and security rules would face hefty fines, with penalties ranging in the tens of millions of Euros.

The GDPR signals Europe's hard stance on data privacy and security at a time when more individuals are committing their personal data to cloud services and security breaches are becoming more common.

- Data transit across borders is handled safely.
- Subjects' consent is required for data processing.
- Requiring certain businesses to employ a data protection officer to supervise GDPR compliance;
- Anonymizing data to safeguard privacy.
- Notifying customers of data breaches

MERCANTILE EXCHANGE HOUSE (UK) LIMITED complies with GDPR data protection laws in order to secure the data of its clients.

Scope:

All customer data, personal data, and other company data are covered by this data security policy. As a result, it applies to every server, database, and IT system that processes such data, as well as any device used for email, web access, or other work-related duties on a regular basis. This policy applies to every user who interacts with the company's IT services.

Out of Scope

This policy does not apply to information that is classified as public. Other data can be omitted from the policy by firm management for specific business reasons, such as the expense or complexity of securing the data.

Policy:

"GDPR Data/Sensitive payment data" refers to information, such as customised security credentials that could be exploited to commit fraud.

All customer data, personal data, and other company data are considered sensitive data. As a result, every server, database, and IT system that processes such data, as well as any device that is commonly used for email, online access, or other work-related duties, is included. This policy applies to every user who interacts with the company's IT services.

All sensitive data must be protected with access controls in order to ensure that it is not improperly disclosed, deleted, updated, or rendered unavailable. Logs must be able to track all access to such data, as well as identify who accessed it and when.

Employees who are in charge of authorisation and have access to secret and sensitive information shall only have access to material at that level or below on a need-to-know basis. System access must be designed to restrict all but a specific user who needs access for their business job.

The data access request process must be followed when accessing systems, devices, or computers that hold confidential, sensitive, or private information. All requests must be approved by the company's MLRO and include a completed authorization request form. Access to data beyond the scope of the employee's approved function must also be granted.

Principles

This Policy aims to ensure compliance with the Laws. UK UK-GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by UKUK-GDPR in order to safeguard the rights and freedoms of the data subject.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures

Data Collection:

Before conducting a transaction or signing up a new customer, the corporation collects all forms of personal information for the aim of due diligence and to meet legal obligations.

Personal details

- Full Name
- Date of birth
- Home Address
- Email
- Contact number (preferred mobile)

Identity Documents

- Photo ID (Such as Passport, Driving Licence and National ID card)
- Customer live photo for face match with ID image
- Address proof (Such as utility bill or Bank Statement)

Payment data

- Currency sell and buy
- Currency send and receive
- Purpose of transfer

Beneficiary Details

- Full Name
- Receiving country
- Account Number
- Bank Name
- Payment reference

The Right of Data Subjects

UKUK-GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

1. The right to be informed (Part 12).
2. The right of access (Part 13);
3. The right to rectification (Part 14);
4. The right to erasure (also known as the 'right to be forgotten') (Part 15);
5. The right to restrict processing (Part 16);
6. The right to data portability (Part 17);

7. The right to object (Part 18); and
8. Rights with respect to automated decision-making and profiling (Parts 19 and 20).

User Authorization and Control:

Users:

The use of non-authenticated user IDs or user IDs that are not related with a single recognised user is forbidden.

For access to MERCANTILE EXCHANGE HOUSE (UK) LIMITED information systems and networks, each user must use a unique user ID and a personal secret password.

Access privileges for each user must be approved based on business needs, restricted to the bare minimum required to complete job tasks, and assigned based on job categorization and function.

Systems:

To authenticate all system users, each computer system must have an automated access control mechanism. This process must:

- If the chosen ID is already in use, the digit 1 should be inserted at the end. Identify each user using a unique user identifier (user ID) MERCANTILE EXCHANGE HOUSE (UK) LIMITED employer user IDs will consist of the employee's first initial followed by the last name.
- Require that new passwords cannot be the same as the four previously used passwords
- Lock-out accounts after not more than six invalid logs on
- Require system idle time out of 15 minutes.
- Require passwords to be reset at least every 90 days
- Encrypt all passwords during transmission and storage on all system components
- Remove or disable inactive users at least every 90 days.
- Require that once a user account is locked out, it remains locked for thirty minutes or until the system administrator resets the account.

Reporting Requirements:

The management requires a certain form of report, which includes:

- Monthly report reflecting the percentage of devices that are compliant
- Weekly incident reports to management
- High-risk situations that are discovered by IT and should be reported to a higher authority as soon as possible.

Employee Requirements:

- Staff must get security awareness training and agree to follow the acceptable use policy if they encounter an unknown, un-escorted, or otherwise unauthorised

individual on corporate property.

- Staffs are prohibited from discussing the subject or substance of sensitive or secret data in public or through systems or communication channels that were not under the company's control. It is not permitted, for example, to distribute data via external e-mail systems that are not hosted by us.
- Employees must ensure that all printed in scope data is not left unattended at the workstation in order to maintain information security.
- At employee's workstation, in scope data is not left unattended.
- According to the password policy, a safe password must be employed on all platforms. These credentials must be one-of-a-kind and cannot be used on any other systems or services.
- Terminated employees will be obliged to surrender all records containing personal information, regardless of format.
- In the event that a device containing in scope data is lost, staff must promptly alert management (e.g. mobiles, laptops etc.).
- If you or a member of your team discovers a system or process that you believe is in violation of this policy or the information security objective, you have a responsibility to notify management so that they can take appropriate action.
- Data that needs to be transported within the company should only be done so using secure transfer protocols offered by the enterprise (e.g. encrypted USB keys, file shares, email etc.). Other procedures must not be used to handle data that is out of scope. If you have a question about how to use a transfer mechanism or if it doesn't satisfy your business needs, you should contact a higher authority.
- Any data transferred on a portable device (such as a USB stick or a laptop) must be encrypted in accordance with industry best practices and applicable laws and regulations. If you're unsure about the requirements, ask for help from management.

Actions:

MERCANTILE EXCHANGE HOUSE (UK) LIMITED must take the following course of action:

- Create secure networks to protect online data from hacks and malware
- Include contract clauses or communicate statements on how we handle data
- Restrict and monitor access to sensitive data
- Establish data protection practices
- Train employees in online privacy and security measures
- Include contract clauses or communicate statements on how we handle data

Lawful, Fair and transparent Data Processing

1. UKUK-GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. UKUKGDPR states that processing of personal data shall be lawful if at least one of the following applies:
 - i. The data subject has given consent to the processing of their personal data for one or more specific purposes;
 - ii. The processing is necessary for the performance of a contract to which

- the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- iii. The processing is necessary for compliance with a legal obligation to which the data controller is subject;
 - iv. The processing is necessary to protect the vital interests of the data subject or of another natural person;
 - v. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
 - vi. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
2. If the personal data in question is “special category data” (also known as “sensitive personal data”) (for example, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:
- i. The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
 - ii. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law;
 - iii. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
 - iv. The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
 - v. The processing relates to personal data which is clearly made public by the data subject;
 - vi. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
 - vii. The processing is necessary for substantial public interest reasons which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
 - viii. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an

employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of the law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK-GDPR;

- ix. The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of the law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
- x. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK-GDPR based on the law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Specified, Explicit and legitimate Purpose

- i. MERCANTILE EXCHANGE HOUSE (UK) LIMITED collects and processes the personal data set out in Part 21 of this Policy. This includes:
 - a. Personal data collected directly from data subjects; and
 - b. Personal data obtained from third parties.
- ii. MERCANTILE EXCHANGE HOUSE (UK) LIMITED only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the UK-GDPR).
- iii. Data subjects are kept informed at all times of the purpose or purposes for which MERCANTILE EXCHANGE HOUSE (UK) LIMITED uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

Profiling

- a. MERCANTILE EXCHANGE HOUSE (UK) LIMITED may use personal data for profiling purposes.
- b. When personal data is used for profiling purposes, the following shall apply:
 - i. Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;
 - ii. Appropriate mathematical or statistical procedures shall be used;
 - iii. Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
 - iv. All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).

Personal Data Collected, Held and Processed

For details of personal data is collected, held, and processed by MERCANTILE EXCHANGE HOUSE (UK) LIMITED (for details of data retention, please refer to MERCANTILE EXCHANGE HOUSE (UK) LIMITED's Data Retention Policy), please refer to our Data Privacy Notice displayed in our website.

Data Security - Transferring Personal Data and Communications

MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

1. All emails containing personal data must be encrypted; for details of encryption, please refer to our IT Security Policy.
2. All emails containing personal data must be marked "confidential";
3. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
4. Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
5. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted using secure means;
6. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
7. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using approved secure courier services; and
8. All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

Data Security - Storage

MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall ensure that the following measures are taken with respect to the storage of personal data:

1. All electronic copies of personal data should be stored securely using passwords and data encryption;
2. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
3. All personal data stored electronically should be backed up daily with backup's stored offsite. All backups should be encrypted;

4. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smart phones), whether such device belongs to MERCANTILE EXCHANGE HOUSE (UK) LIMITED or otherwise without the formal written approval of the Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
5. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the UK-GDPR (which may include demonstrating to MERCANTILE EXCHANGE HOUSE (UK) LIMITED that all suitable technical and organisational measures have been taken).

Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to MERCANTILE EXCHANGE HOUSE (UK) LIMITED's Data Retention Policy

Data Security - Use of Personal Data

MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall ensure that the following measures are taken with respect to the use of personal data:

1. No personal data may be shared informally and if an employee, agent, subcontractor, or other party working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Officer, Mahmud Hossain Bhuiyan.
2. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED or not, without the authorisation of the data Protection Officer;
3. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
4. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
5. Where personal data held by MERCANTILE EXCHANGE HOUSE (UK) LIMITED is used for marketing purposes, it shall be the responsibility of the Compliance Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS

Data Security - IT Security

MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall ensure that the following measures are taken with respect to IT and information security:

1. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by MERCANTILE EXCHANGE HOUSE (UK) LIMITED is designed to require such passwords;
2. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method;
3. All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. MERCANTILE EXCHANGE HOUSE (UK) LIMITED's IT contractor shall be responsible for installing any and all security-related updates; and
4. No software may be installed on any Partnership-owned computer or device without the prior approval of the IT Contractor.

Record keeping:

MERCANTILE EXCHANGE HOUSE (UK) LIMITED keeps a thorough record of every transaction, including copies of the clients' identification and proof of address. All of these records will be preserved for five years from the date of the most recent transaction.

The company will issue a receipt for each transaction, which is signed by the consumer and kept in the records for five years.

When establishing the business relationship the following information is obtained:

- Beneficiary entire information, including father name, identity card, passport, and address
- Sender complete information, including name, father name, identity card, passport, and post code in relation to payment receiver, as well as sources of funds

Data Protection Impact Assessments

1. MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the UKUK-GDPR.
2. Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
 - i. The type(s) of personal data that will be collected, held, and processed;

- ii. The purpose(s) for which personal data is to be used;
- iii. MERCANTILE EXCHANGE HOUSE (UK) LIMITED's objectives;
- iv. How personal data is to be used;
- v. The parties (internal and/or external) who are to be consulted;
- vi. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- vii. Risks posed to data subjects;
- viii. Risks posed both within and to MERCANTILE EXCHANGE HOUSE (UK) LIMITED; and
- ix. Proposed measures to minimise and handle identified risks.

Data subject Access

1. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which MERCANTILE EXCHANGE HOUSE (UK) LIMITED holds about them, what it is doing with that personal data, and why.
2. Data subjects wishing to make a SAR may do so in writing, using MERCANTILE EXCHANGE HOUSE (UK) LIMITED's Subject Access Request Form, or other written communication. SARs should be addressed to MERCANTILE EXCHANGE HOUSE (UK) LIMITED's Data Protection Officer at Mahmud Hossain Bhuiyan.
3. Responses to SARs shall normally be made within one month of receipt, however
 - a. This may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
4. All SARs received shall be handled by MERCANTILE EXCHANGE HOUSE (UK) LIMITED's Data Protection Officer.
5. MERCANTILE EXCHANGE HOUSE (UK) LIMITED does not charge a fee for the handling of normal SARs. MERCANTILE EXCHANGE HOUSE (UK) LIMITED reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of personal Data

1. Data subjects have the right to require MERCANTILE EXCHANGE HOUSE (UK) LIMITED to rectify any of their personal data that is inaccurate or incomplete.
2. MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing MERCANTILE EXCHANGE HOUSE (UK) LIMITED of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
3. In the event that any affected personal data has been disclosed to third parties,

those parties shall be informed of any rectification that must be made to that personal data

Ensure of personal data

- a. Data subjects have the right to request that MERCANTILE EXCHANGE HOUSE (UK) LIMITED erases the personal data it holds about them in the following circumstances:
 - i. It is no longer necessary for MERCANTILE EXCHANGE HOUSE (UK) LIMITED to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
 - ii. The data subject wishes to withdraw their consent to MERCANTILE EXCHANGE HOUSE (UK) LIMITED holding and processing their personal data;
 - iii. The data subject objects to MERCANTILE EXCHANGE HOUSE (UK) LIMITED holding and processing their personal data (and there is no overriding legitimate interest to allow MERCANTILE EXCHANGE HOUSE (UK) LIMITED to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);
 - iv. The personal data has been processed unlawfully;
 - v. The personal data needs to be erased in order for MERCANTILE EXCHANGE HOUSE (UK) LIMITED to comply with a particular legal obligation;
- b. Unless MERCANTILE EXCHANGE HOUSE (UK) LIMITED has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- c. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).
 - i. Effort to do so).

Restriction of Personal Data Processing

1. Data subjects may request that MERCANTILE EXCHANGE HOUSE (UK) LIMITED ceases processing the personal data it holds about them. If a data subject makes such a request, MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Data portability

1. In some cases, MERCANTILE EXCHANGE HOUSE (UK) LIMITED processes personal data using automated means such as KYC support tools.
2. Where data subjects have given their consent to MERCANTILE EXCHANGE HOUSE (UK) LIMITED to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between MERCANTILE EXCHANGE HOUSE (UK) LIMITED and the data subject, data subjects have the right, under the UKUK-GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).
3. To facilitate the right of data portability, MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall make available all applicable personal data to data subjects in a format, compatible to the information fields MERCANTILE EXCHANGE HOUSE (UK) LIMITED would require to on board a client
4. Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
5. All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

Objections of Personal Data Processing

1. Data subjects have the right to object to MERCANTILE EXCHANGE HOUSE (UK) LIMITED processing their personal data based on legitimate interests.
2. Where a data subject objects to MERCANTILE EXCHANGE HOUSE (UK) LIMITED processing their personal data based on its legitimate interests, MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall cease such processing immediately, unless it can be demonstrated that MERCANTILE EXCHANGE HOUSE (UK) LIMITED's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
3. Where a data subject objects to MERCANTILE EXCHANGE HOUSE (UK) LIMITED processing their personal data for direct marketing purposes, MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall cease such processing immediately.
4. Where a data subject objects to MERCANTILE EXCHANGE HOUSE (UK) LIMITED processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the UKUK-GDPR, "demonstrate grounds relating to his or her particular situation". MERCANTILE EXCHANGE HOUSE (UK) LIMITED is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest

Automated Decision Making

1. MERCANTILE EXCHANGE HOUSE (UK) LIMITED may use personal data in automated decision-making processes to support its KYC obligations under statutory and regulatory obligations applicable to financial services providers.

2. Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the UKGDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from MERCANTILE EXCHANGE HOUSE (UK) LIMITED.
3. The right described in Part 19.2 does not apply in the following circumstances:
 - a. The decision is necessary for the entry into, or performance of, a contract between MERCANTILE EXCHANGE HOUSE (UK) LIMITED and the data subject;
 - b. The decision is authorised by law; or
 - c. The data subject has given their explicit consent

Profiling

1. MERCANTILE EXCHANGE HOUSE (UK) LIMITED may use personal data for profiling purposes.
2. When personal data is used for profiling purposes, the following shall apply:
 - a. Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;
 - b. Appropriate mathematical or statistical procedures shall be used;
 - c. Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
 - d. All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 to 26 of this Policy for more details on data security).

Personal Data Collected, Held and Processed

For details of personal data is collected, held, and processed by MERCANTILE EXCHANGE HOUSE (UK) LIMITED (for details of data retention, please refer to MERCANTILE EXCHANGE HOUSE (UK) LIMITED's Data Retention Policy), please refer to our Data Privacy Notice displayed in our website.

Keeping Data Subject Informed

1. MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall provide the information set out in Part 12.2 to every data subject:
 - a. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
 - b. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
 - i. if the personal data is used to communicate with the data subject,

- when the first communication is made; or
 - ii. if the personal data is to be transferred to another party, before that transfer is made; or
 - iii. as soon as reasonably possible and in any event not more than one month after the personal data is obtained.
2. The following information shall be provided:
- a. Details of MERCANTILE EXCHANGE HOUSE (UK) LIMITED including, but not limited to, the identity of its Data Protection Officer;
 - b. The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
 - c. Where applicable, the legitimate interests upon which MERCANTILE EXCHANGE HOUSE (UK) LIMITED is justifying its collection and processing of the personal data;
 - d. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
 - e. Where the personal data is to be transferred to one or more third parties, details of those parties;
 - f. Where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);
 - g. Details of data retention;
 - h. Details of the data subject's rights under the UK-GDPR;
 - i. Details of the data subject's right to withdraw their consent to MERCANTILE EXCHANGE HOUSE (UK) LIMITED's processing of their personal data at any time;
 - j. Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the UK-GDPR);
 - k. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
 - l. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences

Ownership and Responsibilities:

Employees that have primary responsibility for preserving data that they own, such as an executive, department manager, or team leader, are known as data owners.

MERCANTILE EXCHANGE HOUSE (UK) LIMITED employees shall report any data breach to the company's director and MLRO and the matter will be handled according to the company's security procedures.

Executive directors, department managers, and team leaders are examples of data owners who are primarily accountable for keeping information that they hold.

Restriction of Personal Data Processing

- Data subjects may request that MERCANTILE EXCHANGE HOUSE (UK) LIMITED ceases processing the personal data it holds about them. If a data subject makes such a request, MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
- In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Data Portability

- In some cases, MERCANTILE EXCHANGE HOUSE (UK) LIMITED processes personal data using automated means such as KYC support tools.
- Where data subjects have given their consent to MERCANTILE EXCHANGE HOUSE (UK) LIMITED to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between MERCANTILE EXCHANGE HOUSE (UK) LIMITED and the data subject, data subjects have the right, under the UKUK-GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).
- To facilitate the right of data portability, MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall make available all applicable personal data to data subjects in a format, compatible to the information fields MERCANTILE EXCHANGE HOUSE (UK) LIMITED would require to on board a client
- Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
- All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

Transferring Personal Data to a Country Outside the UK

1. MERCANTILE EXCHANGE HOUSE (UK) LIMITED may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the UK.
2. The transfer of personal data to a country outside of the UK shall take place only if one or more of the following applies:
 - i. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the UK has determined ensures an adequate level of protection for personal data;
 - ii. The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the UK; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification

under an approved certification mechanism (as provided for in the UK-GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

- iii. The transfer is made with the informed consent of the relevant data subject(s);
- iv. The transfer is necessary for the performance of a contract between the data subject and MERCANTILE EXCHANGE HOUSE (UK) LIMITED (or for pre-contractual steps taken at the request of the data subject);
- v. The transfer is necessary for important public interest reasons;
- vi. The transfer is necessary for the conduct of legal claims;
- vii. The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- viii. The transfer is made from a register that, under UK law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register

Data Breach Notification

- a. All personal data breaches must be reported immediately to MERCANTILE EXCHANGE HOUSE (UK) LIMITED's Data Protection Officer (Mahmud Hossain Bhuiyan).
- b. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- c. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- d. Data breach notifications shall include the following information:
 - i. The categories and approximate number of data subjects concerned;
 - ii. The categories and approximate number of personal data records concerned;
 - iii. The name and contact details of MERCANTILE EXCHANGE HOUSE (UK) LIMITED's data protection officer (or other contact point where more information can be obtained);
 - iv. The likely consequences of the breach;

Details of the measures taken, or proposed to be taken, by MERCANTILE EXCHANGE HOUSE (UK) LIMITED to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Organisational Measures

MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

1. All employees, agents, contractors, or other parties working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall be made fully aware of both their individual responsibilities and MERCANTILE EXCHANGE HOUSE (UK) LIMITED's responsibilities under the UKUK-GDPR and under this Policy, and shall be provided with a copy of this Policy;
2. Only employees, agents, sub-contractors, or other parties working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by MERCANTILE EXCHANGE HOUSE (UK) LIMITED;
3. All employees, agents, contractors, or other parties working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED handling personal data will be appropriately trained to do so;
4. All employees, agents, contractors, or other parties working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED handling personal data will be appropriately supervised;
5. All employees, agents, contractors, or other parties working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
6. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
7. All personal data held by MERCANTILE EXCHANGE HOUSE (UK) LIMITED shall be reviewed periodically, as set out in MERCANTILE EXCHANGE HOUSE (UK) LIMITED's Data Retention Policy;
8. The performance of those employees, agents, contractors, or other parties working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED handling personal data shall be regularly evaluated and reviewed;
9. All employees, agents, contractors, or other parties working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED handling personal data will be bound to do so in accordance with the principles of the UKUK-GDPR and this Policy by contract;
10. All agents, contractors, or other parties working on behalf of MERCANTILE EXCHANGE HOUSE (UK) LIMITED handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of MERCANTILE EXCHANGE HOUSE (UK) LIMITED arising out of this Policy and the UKGDPR; and
11. Where any agent, contractor or other party working on behalf of MERCANTILE

EXCHANGE HOUSE (UK) LIMITED handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless MERCANTILE EXCHANGE HOUSE (UK) LIMITED against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Annual Internal Control Program:

MERCANTILE EXCHANGE HOUSE (UK) LIMITED will evaluate the policy's efficacy on an annual basis to verify that the company is meeting its stated goals. Changes in the rules and regulations will be updated on a regular basis, and the personnel will be taught.

In the annual review, the following tasks are completed:

- Re-evaluation and testing of monitoring tools
- Updating documentation and systems to reflect new requirements
- Training all employees
- Changing each user's passwords
- Implementation of the plan