Data Protection Policy

Context and overview

Key details

- Policy prepared by: Leon Clifford
- Reviewed by: JRBN Consulting Ltd
- Approved by management: Alex Baroukh
- Policy became operational on: 23/04/2018
- Next review date: 23/04/2019

Introduction

Thomas Exchange UK Ltd (from now on referred to as TEFX) is legally obligated to gather and use certain information about individuals for the sake of anti-money laundering (AML) and counter terrorist financing (CTF) as well as fraud prevention. These can include customers, suppliers, business contacts, employees and other people the company has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

For the purposes of complying with the Data Protection Act 2018 and GDPR; TEFX applies the following lawful bases for processing your personal data.

1) Processing is necessary for compliance with our legal obligation to which we are subject.
2) Legitimate Interests: processing is necessary for our legitimate interests or the legitimate interests of a third party, provided that individual data subject rights are not overriding.

Why this policy exists

This data protection policy exists to ensure that TEFX:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protect itself from the risks of data breach

Data protection law

The Data Protection Act 2018 describes how organisations – including TEFX – must collect, handle and store personal information. These rules apply regardless of how data is stored be it digitally, on paper, etc. Under the Data Protection, TEFX is obligated to collect and use data fairly, stored safely and not disclosed unlawfully. There are eight important principals that underline the Data Protection Act that state unequivocally that all data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be appropriately protected

8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensues an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of TEFX
- All branches of TEFX
- All staff and volunteers of TEFX
- All contractors, suppliers and other people working on behalf of TEFX

Data protection risks

This policy is here to make sure that TEFX is compliant with the law and provide protection from possible security risks such as:

- Breaches of confidentiality – information being inappropriately released
- Reputational damage – Hackers gain access to company's computer systems and acquire sensitive data
- Fraud – Sensitive data used by an individual to commit fraud

Responsibilities

All employees of TEFX have a responsibility for ensuring that all data collected is stored and handled in accordance with the Data Protection Act 2018 and the GDPR. The senior members of staff will have a larger responsibility of not only the handling the data but also making sure all employees, systems, services and equipment meet acceptable security standards.

General staff guidelines

- All data collected is for TEFX to remain compliant with AML and CTF regulations, only staff members who require this data have access to the systems
- All data is considered confidential, employees need to share data in order to be able to work effectively, however data is not to be shared informally or outside of the company
- All employees receive compliance training when they first join as well as annual refresher training which includes the responsibilities of handling data
- All data must be kept up to date, any expired data is retired. Due to AML and CTF guidelines retired data must be kept for a minimum of five years. Any data that is no longer needed is disposed of safely and securely.
- No data should be taken, emailed or posted outside the office and under no circumstances should the company website be accessed by any other computer other than one belonging to TEFX and its contractors

Data storage

This section documents how and where all collected data is stored, any questions regarding the safe storage of data can be directed to senior management. All physical data is stored in secure locations

onsite only accessible to authorised personnel, this includes data that is stored electronically but printed out or vice versa.

All paper or files:

- Are kept in secure locations away from unauthorised personnel
- Are not left where unauthorised personnel can see them
- That are no longer needed are shredded

Electronically stored data is:

- Password protected
- Encrypted
- Stored on designated servers and only uploaded onto secure cloud computing services
- Sited in a secure location
- Backed up frequently
- Protected by approved security software and firewalls

Certain systems that TEFX use for data storage are not maintained in house, but rather outsourced to our IT specialists and web administers. Similarly certain data may not be stored on site but is accessed via the company website or uploaded onto the cloud each evening in case for retrieval in the event of data loss/damage; all data stored off site is encrypted and only accessible to TEFX. The following companies are liable to the same data protection laws of TEFX and are verified annually:

- HBI Consulting Ltd
- Dataquest

Despite outsourcing certain IT services, TEFX is still liable and does not relinquish responsibility. All data collected by TEFX is its liability regardless of where it is stored onsite or not.

Data use

Customer data is of no personal use to TEFX and is only requested in compliance with AML and CTF regulation. Customer data being accessed within the company puts it at higher risk of loss, corruption and theft.

Customer data:

- Should only be accessed when essential
- Should not be shared informally or outside of the company
- Should never be transferred outside of the EEA
- Should never be saved to personal unauthorised computers

Data accuracy

AML and CTF regulations state that all data handled and stored by TEFX must be as accurate as possible. To make sure that TEFX is as accurate as possible with customer data the following guidelines have been put in place:

- Data should be reviewed regularly to make certain that it is accurate
- It has been made easy for customer s to update us on any changes
- Customer files are updated upon discovery

Disclosing data

In particular circumstances, the Data Protection Act requires us to disclose personal data if requested by law enforcements agencies or government bodies or the legitimate interests of a third party, provided that individual data subject rights are not overriding. Under these circumstances TEFX will disclose the requested data, however all requests will be thoroughly reviewed and legitimised by the MLRO.