Contents

Introduction 2
Purpose 2
Scope 3
What is personal data? 3
Our Policy 4
Transparent 4
Accountability and Governance 4
Data Processing Activities 5
Individual Rights 8
Data Protection Officer 10
Breach Notification 10
Data Security 11

Introduction

As a firm which is authorised and regulated by the Financial Conduct Authority (FCA) we are required to establish and maintain appropriate systems and controls for managing operational risks which can arise from inadequacies or failures in our process and systems.

Appropriate and effective data management controls are recognised as integral to our business, as a failure to meet our data privacy and protection obligations could mean potential customer or indeed employee detriment; significant operational loss; loss of reputation; loss of customers and loss of income which, also, could lead to regulatory censure.

We maintain physical, electronic, and procedural safeguards to protect client and employee personal and non-personal data. We have strict internal policies against unauthorised use or disclosure of data. *Client and employee data is accessible only to employees or other personnel who need it to undertake the specific tasks assigned to them*. Staff members are reminded on a regular basis of their obligations about the confidentiality of client and employee information through employee training and operating procedures. Data must only be given to those who have a verified right to that information.

This policy has been drafted in line with overarching FCA system and control requirements and data protection laws within the United Kingdom and the European Union, which have been refreshed. This includes:

- The EU's General Data Protection Regulation (GDPR/'the Regulation') - https://gdpr-info.eu/.
- The UK's updated Data Protection Act 2018, which is the UK's enactment of GDPR - https://services.parliament.uk/bills/2017-19/dataprotection.html
- Wider EU legislation such as the Privacy and Electronic Communications Regulations (PECR) and future updates.
- Wider guidance from the Information Commissioners Office – www.ico.org.uk

GDPR applies to the processing of information relating to individuals, which is carried out by organisations operating within the European Economic Area (EEA). It also applies to organisations outside the EEA which offer goods or services to individuals located within the EEA. Additional conditions are present when granting access to data to individuals based outside of or copying data to locations outside the EEA.

In implementing this policy, it is necessary to determine where employees are based, from where data is accessed and by whom, and where data is stored and/or transferred to.

Purpose

The purpose of this policy is to set out how we achieve compliance with statutory requirements when processing (i.e. collecting, using, sharing, storing and safeguarding) information that can be used to identify a living individual.

This includes but is not limited to ensuring that we meet the GDPR's overarching principles for the processing of data which set out that personal data shall be:

1) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

4) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
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 are processed ('storage limitation');
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 ('integrity and confidentiality').

Ultimately, we, as the data controller, shall be responsible for, and be able to demonstrate compliance with the above principles.

This policy identifies specific data processing requirements that must be met when processing information that which, whether or not intentionally disclosed, may cause physical or mental harm, embarrassment, reputational damage and/or financial loss to those individuals to whom the information relates.

The policy is also designed to work in conjunction with the following frameworks:

- *Information Security*
- *Breach and Issue management*
- *Risk Management*

Scope

This policy has been adopted by the Board of Directors and applies to everyone involved in our business. For the avoidance of doubt, this includes all officers and beneficial owners of the Company as well as all employees (i.e. permanent, contract, self-employed and temporary staff).

If anyone covered by the scope of this policy statement has any queries, these should be raised with *the Managing Director*.

What is personal data?

This policy is centred on the Processing of information that may identify an individual, either singularly or in an aggregated form. Under data protection legislation this is commonly referred to as being personal data.

Personal data means any information relating to an identified or identifiable natural person (commonly referred to as a data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In a work context additional examples of personal data may include records referring to an employee's performance, staff absence, notes on conduct and disciplinary matters.

Personal data may also contain data that is referred to as Special Category Data. Historically this information was referred to as being sensitive personal data. Special Category Data may include data relating to an individual's:

- Sexual orientation
- Sex life

- Trade union membership
- Political or religious views
- Health data
- Genetic and biometric data, where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not considered as being Special Category Data; however additional conditions apply to its processing.

Our Policy

The aim of this policy is:

1) Ensuring the firm is **Transparent** when processing personal data;
2) Holding individuals **Accountable** to ensure the firm is compliant with GDPR requirements;
3) Managing data privacy risks through a **Governance** model;
4) Ensuring **Data Processing Activities** are documented and assessed for legitimacy;
5) Developing effective processes to ensure the firm responds to **Access Rights** requests within mandated timeframes;
6) Identifying and keeping under review, whether it is necessary to appoint a **Data Protection Officer** and where not formally required, assigning responsibility for data protection/privacy to a senior manager**;**
7) Ensuring the firm can fulfil data **Breach Notification** requirements within the mandated timeframe;
8) Identifying **Data Security** requirements for safeguarding personal data.

Transparent

It is a key requirement that our firm is completely open with our employees and customers about how we collect, generate and use personal data. This is achieved through the following measures:

We communicate our data processing activities to clients, employees, and organisations we share personal data with through the use of:

- *Privacy notices*
- *Contractual agreements*

We shall clearly state:

- *The firm's name, including company registration details*
- *How the data will be collected*
- *The purpose for collecting the data*
- *The category of data*
- *How the data will be used*
- *Who the data will be shared with, including current and potential sub-processors of personal data, which we have appointed or may appoint*
- *Details of any transfers outside the EEA*
- Data subject rights
- For how long the data will be retained
- Internal contact details for data protection queries and/or access right requests
- ICO contact details for complaint purposes

Accountability and Governance

Key requirements are:

- Ensuring the privacy risk is managed in a consistent manner that reflects the importance to data subjects and our firm;
- Ensuring someone is ultimately accountable within our firm for ensuring both compliance with data privacy legislation and that privacy issues have an appropriate level of visibility within the organisation. This is achieved through the following measures:

We have appointed a suitably authorised senior individual who is held accountable for ensuring we are compliant with GDPR requirements – this person will be the Data Privacy representative for the firm; this is *the Managing Director.*

Compliance with this policy is assessed on a periodic basis which is currently every six months at the senior management meeting. Management Information (MI) assessing compliance is discussed at senior management level, with outcomes documented and tracked.

Operational risk issues are managed within the existing risk management framework, detailing the risk issue, an assessment on its potential impact to A) data subjects B) the firm, inherent and residual risk, risk action (accepted / to be mitigated / to be reassessed), risk owner, agreed action, action owner, remediation/review date.

Data Processing Activities

We are required to demonstrate we fully understand our lawful basis for collecting and processing personal data, as well as knowing where personal data is located and accessed from, the purpose for collecting the data, who is using the data, for how long it is necessary to retain the data and communicating our data processing activities to data subjects.

The lawful bases for processing data are:

1) Consent: the individual has given clear consent to process their personal data for a specific purpose.
2) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
3) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).
4) Vital interests: the processing is necessary to protect someone's life.
5) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
6) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Our controls in relation to data processing activities are achieved through the following measures:

We have established and documented the territorial scope (the data processing model) of our data processing activities. Details captured include:

- The location of places of work, calls centres including those IT support staff, who provide application development and maintenance;
- Locations where the personal data is stored;
- Locations where the data is accessed from.

We have determined our lawful bases for processing personal data and have undertaken a data mapping activity that establishes how we collect data, the purpose for collecting the data we use, data users, who it's shared with and for how long it needs to be retained.

Data captured is categorised according to its sensitivity e.g. personal data, special category data, criminal conviction data and categorised according to the legal basis relied upon for collecting the data e.g. the performance of a contract, legitimate interest, consent etc.

We have established that we collect and process data for one or more of the following lawful bases:

1) To fulfil our contract with both our customers and employees**:** We need to use personal data as is necessary to provide our customers with the service and products we have agreed to provide in line with our overall service contract as well as employment contracts.
2) We have a legitimate interest in doing so**:** Taking into account customer interests, we process data to analyse customer behaviour in order to improve our services, offerings and pricing; to track commission or remuneration that may be due to us; to provide for business continuity in the event of interruption or cessation; to provide you with information about our products and services; and to the extent required for the administration of our financial services, to ensure we have appropriate records.
3) We are required to do so by law or regulation**:** We are required by the *FCA (or any other regulatory or legislative body)* to process and store some data in order to fulfil our legal or regulatory obligations. We may capture and share personal data with organisations who can confirm our customers/employees' identity and provide information necessary to prevent fraud or other crimes. We may also be required to share personal data where requested to by legal authorities or the Financial Ombudsman.
4) We have been provided with consent**:** Where customers have provided their informed consent, we will process personal data in accordance with the permission they have given us and will process any withdrawal of consent – personalise as appropriate]
5) We have been provided with explicit consent: Where customers provide their explicit consent, we will process their special categories of data and criminal convictions data in accordance with the permission they have given us and will process any withdrawal of consent.

Where we have collected data through consent, we will:

- Record the collection method
- Record what the data subject has consented to
- Record the individual's name and the date consent was granted
- Record the category of personal data i.e. personal data, special categories of data, data relating to criminal records and/or offences, being processed
- Record whether the consenting individual is a parent or guardian that is providing consent for another
- Provide a method for allowing individuals to withdraw their consent
- For explicit consent we will ensure that the customer has physically written/typed a consenting phrase, such as "I consent to this processing".

Where a requirement exists to transfer or grant access to special categories of personal data, explicit consent to do so must be gained from the data subject prior to the transfer or accessing of the data.

This also documents our data processing activities, commonly referred to as a record of processing. Information captured includes a descriptor of the activity e.g. payroll, the administering of employees, the processing of [claims / quoting / to place business / all of these / etc.], marketing, automated decision making.

Where we use personal data for marketing purposes, we will document:

- The purpose of the marketing activity

- The legal basis we use to process the personal data
- Where we receive the data from third parties and if so confirmation from the third party that a legal basis for sharing the exists and what that is
- Where we collect personal data directly from individuals, how the data was captured and how its intended use was communicated to those individuals that the information relates to

In addition:

- Depending on how the data is collected / captured e.g. place business / quote for business / contact form we have determined a 'reasonable' amount of time to retain and continue to use the data. The records of our data processing activities set out the data retention periods we have set for different types of data.
- Where we process special categories and criminal conviction data, for the performance of our contract and under the condition of consent we will ensure that the appropriate additional safeguards are in place to protect the data, these will include added security measures, restriction in access to the data. We will also ensure that we will only process the data for as long as is necessary for the purposes we have collected it and will endeavour to erase the data securely at the earliest opportunity, whilst also ensuring that we continue to meet our obligations as a data controller
- We also check the data for accuracy; and
- Where consent is used for processing personal data we have a process to allow individuals to object to being contacted and to stop further communications.

Where we utilise an automated decision-making mechanism to identify who to market our products to, the suitability of individuals to buy our products and/or price products, we document:

- The purpose of the automated decision activity
- Whether an alternative manual method is available to perform this activity
- How the use of this technology is communicated to data subjects e.g. through a privacy notice, clearly stating why the use of this mechanism is necessary

Where we undertake profiling activities, we document:

- The reason for profiling
- The profiling method
- Whether any automated means are used when performing the profiling activity
- The outcome (including impact on the data subject) of the profiling activity e.g. may result in increases / decreases in premium if using telematics. Other profiling examples follow:
  - internet search and browsing history
  - data derived from existing customer relationships
  - data collected for creditworthiness assessments
  - financial and payment data
  - consumer complaints or queries
  - other locational data that may be collected through smart applications

Where we use third party processors or outsourcers (including hosted online services) including IT service providers, we shall document:

- The name of the supplier
- A description of the services being provided e.g. to provide payroll services
- The operational reliance on the provider
- The location of the third party
- The category of data being accessed

- Whether access is onsite / offsite
- If offsite, the method of access
- If the data is externally hosted (cloud based), the name and platform of the provider
- Whether the supplier requires copies of data for application support, development of maintenance purposes
- If he supplier transfers the data internationally
- A description of technical, physical and organisational controls to safeguard the data
- If requiring copies of personal data:
  - Whether an understanding has been gained on third party technical and organisational data safeguarding measures
  - Whether data ownership, uses, agreed and approved data storage locations are documented within the contractual arrangements
  - Document within the contract what should happens to the data at the end of any contractual arrangement

Individual Rights

The GDPR and UK data protection law grants data subject specific rights of access where their personal data is being processed. Key requirements centre on individuals being able to request information being held, for what purpose, how the data was gathered, who the data is shared with, where the data is located, how the data is safeguarded, to request the rectification and the deletion of data and to object to the processing of data, including preventing further processing. Specific rights are as follows:

1) Information to be provided where personal data are collected from the data subject;

This requirement focuses on the collection / creation of personal data. Compliance is achieved through the use of privacy notices, outlining privacy requirements within terms of business, commercial contracts and contracts of employment.

2) Information to be provided where personal data has not been obtained from the data subject; Additional requirements are present when receiving personal data from other parties, these are:
   - Setting out the categories of personal data
   - The source where the personal data originates from and whether it came from publicly accessible sources

   Privacy notices should highlight the use of these third parties, stating the reason for using the third party.

3) Right of access

   Data subjects have the right to request details on what information is being held on about them, for what purpose, how the data is used, how long the data is retained for, who it is shared with and whether the data is transferred abroad. It is likely most requests from data subjects will centre on the data being held and purpose. Compliance is achieved by validating requests and the identity of the individual making the request and to responding to requests within the mandated timeframe. See appendix A for details on process requirements.

4) Right to rectification

   Data subjects have the right to request that any data held on them is rectified if inaccurate or incomplete. Compliance is achieved by validating requests and the identity of the individual

making the request and preventing further processing whilst the inaccurate data is rectified. See appendix B for details on the handling process.

5) Right to erasure ('right to be forgotten')

   Data subjects have the right to request that any data held on them is deleted however this does not necessarily mean that the data needs to be deleted. In processing such requests, we will consider our lawful basis for retaining such data and the consequences on the services we provide of deleting such data, if any. Requests should be acted on as soon as they are received. See appendix C for details on the handling process.

6) Right to restrict processing

   Data subjects have the right to request that data processing is restricted if the data is no longer required for its original purpose, the data collected is excessive for its purpose, the processing is unlawful or the data is inaccurate. See appendix D for details on the handling process.

7) Right to data portability

   Data subjects have the right to request that any personal data relating to them is provided to them in a machine-readable format. Organisations are under no obligation to import any that has been provided to a data subject in this way. We shall determine likely circumstances where individuals might exercise the portability right.

8) Right to object

   Data subjects have the right to object to the processing of personal data relating to them, particularly where the personal data is being used for profiling and/or marketing purposes. Where valid and no lawful basis exists for continuing to process the data, we are required to prevent further processing of the data. See appendix E for details on the handling process.

9) Right to be informed about automated individual decision-making, including profiling

   Data subjects have right to be informed on activities where automated decision making or profiling is performed on their data. Compliance is achieved through the use of privacy notices, outlining privacy requirements within TOBAS, commercial contracts and contracts of employment. See appendix F for details on the handling process.

We will maintain a register of requests from data subjects and third parties about data subjects' individual rights:

- The date the request was received
- How the request was received
- The name of the individual making the request
- Method used for confirming the individual's identity
- Whether the request is legitimate or not
- If not legitimate, then documenting why not
- Documenting any circumstances where the Company is unable to fulfil or part-meet the request
- Next steps
- Response date
- Closure date

Data subjects have the right to be informed when the data relating to them has been rectified, restricted or erased. As part of our processes and procedures we shall determine likely scenarios where we are required to comply with this right.

Data Protection Officer

Certain organisations are required to appoint a Data Protection Officer. The appointing of a DPO centres on the volume of personal data being processed, the category of data being processed and the processing activity.

Organisations must appoint a DPO if they:

- *Carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or*
- *Carry out large scale processing of special categories of data or data relating to criminal convictions and offences.*

We have reviewed the regulations and associated guidance and have determined that we are not required to appoint a formal Data Protection Officer. However, to ensure appropriate accountability and governance, we feel it is appropriate to appoint **a Data Protection Representative** to ensure compliance with GDPR obligations and this role is fulfilled by the Managing Director.

When requested, employees shall fully co-operate with requests for assistance. Non-cooperation may be treated as a disciplinary offence.

Breach Notification

Key requirements centre on the ability to assess impact and to report 'material' data loss incidents to the Information Commissioner's Office within 24-72 hours (not working hours) of becoming aware of the event. Where the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we are required to inform data subjects without undue delay.

We maintain a data breach management process that includes the following:

1) A point of contact to report data security and data loss incidences to.

2) A central log to record the data breach incident detailing:
   - What has happened
   - How and when the firm became aware
   - The category of data
   - The significance of the incident (this is determined by the category of data that has been lost)
   - Potential impact to the Company and data subjects
   - Initial actions including timescales
   - Next steps, including whether data subjects and the relevant supervisory authority need to be informed, including timescales
   - Follow-up actions
3) Agreed lines of escalation and communication for serious data breach issues;
4) Contact details for those who are the first point of contact and escalation points, including out of hours contact details;
5) Where appropriate a rota detailing on-duty first points of contact;
6) Where the Company is required to notify the ICO the following information will be provided:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned;
- The name and contact details of the **Data Protection Representative** where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Those responding to the breach are authorised to immediately perform or to request an immediate containment activity to lessen the impact of the breach e.g. where an IT system is being compromised or data is exposed.

As part of our wider breach management process, we will also consider whether it is appropriate to notify the Financial Conduct Authority (FCA) under both Principle 11 – transparent and open communications with the Regulator - but also whether the breach may be regarded as a notifiable breach due to both the nature and size of the breach. See the separate breach management process for further details.

Examples of data breaches include:

- The accessing of personal data by an unauthorised third party;
- The sending of personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- The loss of availability of personal data.

Data Security

Key requirements centre on organisations implementing data security controls which safeguard personal data, commonly this is known as the data security model. Controls may vary according to the size of the organisation, its commercial activities, and the volume of personal data being processed and the category of personal data.

We have implemented appropriate technical and organisational data security controls to protect the confidentiality, integrity and availability of personal data. Our controls include the following: –

- Encrypting data during transit (as it's being communicated and/or physically transported from one location to another);
- Encrypting data at rest i.e. where data is stored. Examples include data held on data backup tapes, on file servers, laptops, workstations and so-called smart appliances. N.B. Personal data that is stored in the cloud or hosted externally should also be encrypted;
- Restricting access to data to authorised users for approved purposes;
- Periodically security testing applications, services and infrastructure for vulnerabilities, known exploits and configuration errors;
- Maintaining a staff leavers process that removes access to IT services (including cloud and hosted services) on an agreed date;
- Maintaining a clear desk policy where paper-based materials are secured at the end of the working day or during periods of prolonged absence;
- Securely shredding paper-based materials;
- Securely disposing of equipment containing personal data at the end of their intended purpose or following mechanical failure e.g. data held on workstations, laptops, servers, printers and scanners;

- Erasing data at the end of its intended purposes, including activities where computer equipment is assigned from one user to another].