Data Protection and Record Retention Policy

1. Introduction

Unicorn Asset Management (Unicorn) has a legal requirement to follow the Data Protection Act 1998 (DPA), in addition to the requirements under the Financial Conduct Authority's (FCA) rules.

Unicorn is classified as a 'Data Controller' and as such is registered with the Information Commissioners Office (ICO) and recorded on the Data Protection Register under registration number **Z6003682.**

The purpose of this policy is to set out an overview of the DPA, as well as setting out clear practical requirements for its application in respect of the activities of UAM and its staff. If staff are in any doubt as to the application of the DPA requirements, they should contact Compliance.

2. Data Protection Act

The Act regulates how personal information is used and organisations are required to comply with the eight principles or rules of good information handling. These principles state that personal data must be:

- Fairly and lawfully processed
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and where necessary kept up to date
- Not kept longer than is necessary
- Processed in line with the rights of the individual
- Kept secure
- Not transferred to countries outside the European Economic Area unless there is adequate protection for the information
- Compliant with the individual's requests to be forgotten.

The Data Principles are enforceable and all employees must observe, follow and comply with them.

The ICO is an independent public body set up to promote access to official information and to protect personal information. Enforcement of the Data Protection Act 1998 is the responsibility of the ICO.

3. Use of Personal Information

Personal information must be used fairly and lawfully and this is one of the fundamental provisions of the Act. Individuals must be informed for what purpose(s) their personal information is being used. It is important that the use of personal information does not contravene any other laws.

When obtaining personal information, organisations must inform individuals of:

- the name of the business or organisation
- the purpose for which their information will be used
- any other information needed to ensure the use of their personal information is fair

Individuals must be told that they have a right to access their information and have it corrected if it is factually inaccurate. If the information is likely to be used in a way that a person might not expect, this must be disclosed. For example, if the information may be passed to other organisations or if it might be put on file at credit reference agencies.

Similarly, if the individual had been told that they would only receive direct marketing about a firm's own products and services, that firm must not pass the individual's details to another organisation. It is acceptable to send a brochure about similar products to a customer unless they had objected to being sent marketing material.

Typically, it is not permitted to pass individuals' information to another business or organisation unless they have been told this will happen. The exceptions to this are:

- Disclosure to the police if notifying the individual would be likely to prejudice the investigation or prevention of a crime
- Disclosures can also be made if they are necessary for a court case or to obtain legal advice

4. Subject Access Rights

This gives individuals the right to obtain information held about them and includes:

- Whether the organisation, or someone on its behalf, is processing personal information about them
- The information that is being processed, why it is being processed and to whom it may be disclosed
- Receiving a copy of the personal information about them
- The sources of the information

To obtain these details, an individual must send a written or an electronic request, known as a '**subject access request'.** In cases of doubt, the recipient of **subject access request is entitled to ask for proof of identity before responding and any** additional information that might be needed to respond.

The response to a **subject access request must be sent** as soon as possible; in any event no later than forty days after receiving the request. This timescale does not commence until any additional required details have been received. Information must be supplied in a permanent format (computer printout or letter or form) agreed otherwise. If it is not possible in this format, or it can be demonstrated that

it will involve a "disproportionate effort", access must be provided in another way. The information must be clear; i.e. no jargon.

In the event that such a request is received, you must ensure that it is immediately forwarded on to the Compliance Officer for consideration.

5. Staff Requirements

All data relating to personal information, whether customers or employees must be processed and stored in compliance with Data Protection Act legislation. This includes ensuring that the details are kept confidential and are stored securely.

Data must be kept no longer than is necessary and must also be held and maintained in line with FCA or other regulatory requirements. Disposal of data must also be in a secure and compliant manner.

The majority of information is securely held electronically, but where any client and company confidential data is captured in hard copy it should be securely stored in a lockable cabinet or pedestal. Additionally, computer monitors should be locked when a staff member will be losing sight of their PC to prevent unauthorised access to logged in machines.

6. Breaches

Breaches of Data Protection procedures and requirements may be discovered in a number of ways including:

- through normal business processes/daily routine
- findings of a Compliance Monitoring Test
- a complaint or communication from a customer
- an inspection during a third party visit
- as a result of a visit or investigation by the FCA
- an inspection by HMRC

Breaches must be notified to the Compliance team immediately and logged in the breaches register. The breach must then be promptly corrected in accordance with the requirements set out in the Compliance Manual and the Breaches procedures and the circumstances considered to minimise the likelihood of a reoccurrence.

7. Record Retention

Unicorn keeps orderly records of its business and internal organisation, including all services and transactions undertaken by it. All services and transaction records are retained in files, which are maintained for a minimum of 5 years. The record is maintained in a medium which is sufficiently accessible to enable the firm’s activities to be monitored by the FCA.

Unicorn has made arrangements to retain records relating to its business that are:

- Capable of being produced on paper in English
- Readily accessible within 48 hours
- Sufficient to show each key stage of a business transaction
- Sufficient to provide a complete audit trail, that is, evidencing each transaction and any actions taken by Unicorn
- Sufficient to show the internal organisation including implementation of the systems and controls set out in the Compliance Manual and other internal policies and procedures

When records have reached the end of their retention period they must be destroyed. For all electronic records this involves them being completely wiped from systems and fully deleted. This includes any back-up copies on any separate servers or systems.

8. Building Security

Unicorn's office is only accessible by those staff with a key to the main gate of the building complex. The complex is gated with a guard who requires any guests to sign in. Only permanent staff are issued with a key to the building and there are also CCTV cameras around the building complex.