Veritas
— Asset
Management

Real Return
Investing

Veritas Asset Management LLP

Data Protection Policy

December 2020

Veritas Asset Management LLP
1 Smart's Place, London WC2B 5LW

T +44 (0)20 3758 9900
F +44 (0)20 3070 0990
investorservices@vamllp.com
vamllp.com

Introduction

Veritas Asset Management LLP (hereinafter referred to as "VAM", "we", "us" "our") is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data about our staff, clients, suppliers, counterparties and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the General Counsel be consulted before any significant new data processing activity via a third party is initiated to ensure that relevant compliance steps are addressed.

Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: • Compliance with our legal, regulatory and corporate governance obligations and good practice • Providing the services that we have contracted to provide to investors • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests • Ensuring business policies are adhered to (such as policies covering email and internet use) • Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking • Investigating complaints • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments • Monitoring staff conduct, disciplinary matters • Improving services • Marketing our business
Personal data	*'Personal data'* means any information relating to an identified or identifiable natural person ('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.
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	*'Data controller'* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

Processing	*'Processing'* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for VAM is the Information Commissioners Office ("ICO").

Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

VAM's General Counsel has overall responsibility for the day-to-day implementation of this policy. You should contact the General Counsel for further information about this policy if necessary.

The Principles

VAM shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulations. We will make every effort possible in everything we do to comply with these principles. The Principles are:

1. **Lawful, fair and transparent:** Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.
2. **Limited for its purpose:** Data can only be collected for a specific purpose.
3. **Data minimisation:** Any data collected must be necessary and not excessive for its purpose.
4. **Accurate:** The data we hold must be accurate and kept up to date.
5. **Retention:** We cannot store data longer than necessary.
6. **Integrity and confidentiality:** The data we hold must be kept safe and secure.

Accountability and transparency

We must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. We are responsible for keeping a written record of how all the data processing activities that we are responsible for, comply with each of the Principles. This must be kept up to date and must be approved by the General Counsel.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening. Staff data will be dealt with separately as the consent rules are different for such data.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased

Controlling vs. processing data

VAM is classified as a data controller and data processor – please refer to the definitions above.

As a data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing without the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller. As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

If you are in any doubt about how we handle data, contact the General Counsel for clarification.

Lawful basis for processing data

We must establish a lawful basis for processing data. Ensure that any data you are responsible for managing has a written lawful basis approved by the General Counsel. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent:** Where appropriate, we hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
2. **Contract:** The processing is necessary to fulfil or prepare a contract for the individual.
3. **Legal and regulatory obligation**: We have a legal obligation to process the data (excluding a contract)
4. **Vital interests:** Processing the data is necessary to protect a person's life or in a medical situation.
5. **Public function:** Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
6. **Legitimate interest**: The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which condition to rely on

If you are making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the General Counsel.

Special categories of personal data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics

- Biometrics (where used for ID purposes)
- Health
- Sexual orientation

In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

Responsibilities

The Firm's responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

Your responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy and any related policies at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay
- Keep your own personal data up to date via the Human Resources Management System (HRMS)
- Only access personal data that you have an authorised purpose to access
- Do not disclose data to third parties unless you and they are authorised to have access to such information
- Keep data secure, for example by complying with rules on access to premises, computer access, including password protection and secure file storage and destruction

- Do not remove personal data, or devices containing or that can be used to access personal data, from the Firm's premises without adopting appropriate security measures to secure the data and the device
- Do not store non-work related personal data on local drives or personal devices that are provided for work purposes

Responsibilities of the General Counsel

- Keeping the Managing Partners Board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members
- Answering all questions on data protection
- Responding to individuals such as clients and staff who wish to know which data is being held on them by us
- Checking and approving third parties that handle VAM's data and contracts or agreement regarding data processing

Responsibilities of the Human Resources Director

- Ensure correct access rights are in place with regard to Human Resources Management System and hard copy files
- Ensure hard copy files are kept securely
- Ensure that correct procedures are adhered to when engaging with a new third party data controller or processor in relation to staff data
- Dealing with data protection queries from Staff and processing subject access requests as appropriate
- Ensure an appropriate Recruitment Data Retention Guide is in place
- Ensuring appropriate deletion and retention of ex-staff personal data

Responsibilities of the IT Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services VAM is considering using to store or process data

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the General Counsel.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the General Counsel will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- The Head of IT must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with VAM's backup procedures
- Data should never be saved down directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software
- All possible technical measures must be put in place to keep data secure

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention policies.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data outside of the European Union, or anywhere else outside of normal rules and procedures without express permission from the General Counsel.

Third parties

Using third party controllers and processors

As a data controller (and/or) data processor, we must have written contracts in place with any third party data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Contracts

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

Criminal offence data

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and will be treated as such.

Audits, monitoring and training

Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as defined by the General Counsel and normal procedures.

Monitoring

Everyone must observe this policy. The General Counsel has overall responsibility for this policy. VAM will keep this policy under review and amend or change it as required. You must notify the General Counsel of any breaches of this policy. You must comply with this policy fully and at all times.

Training

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the General Counsel.

Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. VAM has a legal obligation to report any data breaches to the ICO within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both you and VAM at risk.

The importance of this policy means that failure to comply with any requirement may amount to a disciplinary offence, which will be dealt with under the Firm's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing staff or client personal data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the General Counsel.

Please confirm that you have read and accept this policy via the relevant Read and Accept option as instructed via email or on Octopus, or by signing the acknowledgement below.

....

Signed by **Date**