VICTORIA MUTUAL FINANCE LIMITED

VICTORIA MUTUAL
FINANCE LIMITED

DATA PROTECTION POLICY

PAGE OF CONTENTS

1. INTRODUCTION

This Compliance System has been prepared for us by Scott Robert and is specific to Victoria Mutual Finance Limited's (VMFL) data compliance arrangements.

Scott Robert is a trading name of Compliance Consult and Advisory Limited. The company provides a range of regulatory compliance solutions to both businesses and regulators.

The content contained herein has been tailored to VMFL's requirements taking account of information provided by the key people recorded in this document.

The Policies and Procedures section deals with different aspects of our operational activity and sets out the current compliance arrangements in respect of the same. However, we must also operate operational processes and controls to ensure that the compliance arrangements are fulfilled. The operational processes and controls are only contained in this system in part and reference should be made to our operational procedures for further information.

Risk assessments were conducted which took into account anticipated risks arising from our current activity pertaining to our handling of personal and/or sensitive data. We will conduct risk assessments regularly on an ongoing basis and will implement control mechanisms accordingly.

1.1 OVERVIEW OF REGULATORY REQUIREMENTS

Data and the utilisation of data is instrumental to the day to day operations of much of the UK economy. Data often relates to the individuals from whom it was collected, and the law provides those individuals with protection against the misuse of their data. Those who process data, and those who choose how data is processed are under legal obligations to ensure their engagement with data is lawful. The Data Protection Act 1998 ("DPA") provided a comprehensive regulatory regime of data protection in the UK. However, the act was introduced at a time when the modern climate of data dependency was unimaginable. As such, the General Data Protection Regulation ("GDPR") has been implemented to update data protection legislation and bring it in to line with the current data use across the European Union. GDPR will come into force on 25th May 2018.

The GDPR builds upon and extends many of the existing requirements currently in place under the DPA. These changes focus upon revising the expectations upon data controllers and processors, by providing individuals with greater control over how their data is collected and processed. Some of the key changes include increased focus on accountability, the revised definition of consent, the creation of direct rights including the right to be informed, the right to object and the right to erasure, and further powers for the Information Commissioner's Office ("ICO") as the regulatory body for ensuring compliance with the GDPR.

The regulatory requirements under the DPA and the GDPR require organisations to consider whether they are appropriately collecting and processing data before and during data utilisation. Following the introduction of the GDPR, considerable changes will be noticeable for organisations who control or process data.

The requirements of the GDPR will also be perceptible in the provision of data subjects (individuals to whom data relates) with certain rights that they may exercise over the usage of their data. These rights include the right to be informed, the right to object, the right to access and the right to be forgotten (the right to of erasure). The introduction of these rights will create noticeable changes for organisations who seek to collect or process data. The right to be informed, for example, ensures that individuals are provided with information relating to the processing of their data prior to that processing. By providing these rights to individuals, the GDPR increases the regulatory requirements upon organisations and provides individuals with greater control over the usage of their data.

1.2 INTRODUCTION TO THE INFORMATION COMMISSIONER'S OFFICE (ICO)

Data and the utilisation of data is instrumental to the day to day operations of much of the UK economy. Data, often relates to the individuals from whom it was collected, and the law provides those individuals with protection against the misuse of their data. Those who process data, and those who choose how data is processed are under legal obligations to ensure their engagement with data is lawful.

The Data Protection Act 1998 ("DPA") provided a comprehensive regulatory regime of data protection in the UK. However, the act was introduced at a time when the modern climate of data dependency was unimaginable. As such, the General Data Protection Regulation ("GDPR") has been implemented to update data protection legislation and bring it in to line with the current data use across the European Union. GDPR came into force on 25th May 2018.

The GDPR builds upon and extends many of the existing requirements currently in place under the DPA. These changes focus upon revising the expectations upon data controllers and processors, by providing individuals with greater control over how their data is collected and processed. Some of the key changes include increased focus on accountability, the revised definition of consent, the creation of direct rights including the right to be informed, the right to object and the right to erasure, and further powers for the Information Commissioner's Office ("ICO") as the regulatory body for ensuring compliance with the GDPR.

The regulatory requirements under the DPA and the GDPR require organisations to consider whether they are appropriately collecting and processing data before and during data utilisation. Following the introduction of the GDPR, considerable changes will be noticeable for organisations who control or process data.

The requirements of the GDPR will also be perceptible in the provision of data subjects (individuals to whom data relates) with certain rights that they may exercise over the usage of their data. These rights include the right to be informed, the right to object, the right to access and the right to be forgotten (the right to of erasure). The introduction of these rights will create noticeable changes for organisations who seek to collect or process data. The right to be informed, for example, ensures that individuals are provided with information relating to the processing of their data prior to that processing. By providing these rights to individuals, the GDPR increases the regulatory requirements upon organisations and provides individuals with greater control over the usage of their data

2. POLICIES AND PROCEDURES – DATA PROTECTION

These policies and procedures collectively form our regulatory risk management system to ensure that we conduct our business model in accordance to the rules and all relevant laws and regulations. When creating this Compliance System we took into consideration the risk areas identified from our Regulatory Risk Assessment and have created the following policies and procedures as a mechanism to ensure that we minimise the probability of the regulatory risk materialising.

We regularly review the adequacy of our regulatory risk management system by way of monitoring our risks, KPI's and MI to ensure that we are operating effectively and that amendments are made to rectify any inadequacies identified.

2.1 GOVERNANCE AND ACCOUNTABILITY POLICY AND PROCEDURE – INTRODUCTION

Our company understands and accepts the requirements placed upon us by the GDPR.

We have identified potential risks and implemented procedures to ensure our ongoing compliance with the legislation, ensuring that our company has the necessary structure, efficacy of accountability, monitoring, collection and utilisation of management information as well as the appropriate complaints procedures.

We are confident in our ability to operate in conformity with the regulatory requirements that apply by virtue of our authorisation with our regulator, both at this present time and in the event of any change to our business.

2.2 FIRM GOVERNANCE

To assist in setting out our governance arrangements we have separated each area of potential concern into its own category, detailing the measures we have implemented and the risk each of those measures is intended to address.

Clear directorial responsibilities

We will ensure our director's responsibilities, specifically in relation to data, are clearly documented with each director signing an acknowledgement that they have understood their responsibilities. At least one individual is responsible for dealing with the apportionment of responsibility for data protection. These measures ensure that directors can be held accountable for their acts or omissions whilst business affairs can be monitored and controlled.

Clear reporting lines

We will have in place, a documented structure chart, which details the clear reporting lines between our board, senior management, and specific departments and that document is reviewed bi-annually. Senior management can thereby ensure that they are aware of their responsibilities.

Clear and appropriate apportionment -

We will ensure, on a quarterly basis, the individual responsible for apportionment of responsibilities reviews and reapportions those responsibilities appropriately. This ensures that significant responsibilities are regularly reviewed, that responsibilities are apportioned in conjunction with the firms' growth and that it mitigates against the risk of failures caused by unclear apportionment.

Strong senior management structure with appropriate monitoring of director responsibilities -

We will ensure those invited to attend management meetings are notified in advance, management meeting minutes are taken and distributed to attendees and a quorum has been implemented to ensure decisions are made based on a minimum number of votes. This ensures that directors make decisions based on the customer's best interest and wherever a decision is made which may not be in the best interest of the firm, such a decision can be challenged.

Systems and controls enable the firm to monitor and ensure compliance -

We will fully implement this manual which contains extensive policies and procedures in relation to our use of data. We are aware that the compliance manual must be reviewed and updated on a quarterly basis. Individuals are appointed to oversee the firm's compliance, they are responsible for monitoring our compliance and reports to the board monthly. As part of the management meeting agenda the Board discusses any issues, concerns or general information regarding compliance. These measures enable the firm to monitor, identify and assess compliance risks. They also ensure that we minimise the risk of conducting activity that is in breach of the ICO regulations and the risk of regulatory action being taken against us.

Management information is gathered appropriately –

We will have a system is in place that details the required information, when that information is required and for whom it is required. Management information is then included on management meeting agendas with the minutes of the meeting recorded and stored. Through these steps, we have addressed the risk of being unable to identify, monitor or manage risks of regulatory concern, such as the fair treatment of our customers.

Proper assessments of responsible employee's honesty and competence –

We will ensure individuals within the firm are assessed at the point of recruitment to ensure their suitability. Additionally, a clear and documented recruitment process is in place. Through this we ensure that our employees can fulfil the role competently and that they neither act dishonestly nor treat customers unfairly.

Procedures in place to ensure senior management implement and maintain the business continuity policy –

We will ensure we have in place a business continuity plan which documents the key business risks and mitigations in the event of those risks occurring. Our business continuity plan is reviewed annually, mitigating against the potential risks that the business activity becomes disrupted which could cause the firm to lose revenue, have a detrimental impact to customers if services are disrupted as well as increase the potential loss of essential data.

Our firm appropriately assesses the requirement for a Data Protection Officer –

We will assess the requirement and decide whether to appoint or outsource a Data Protection Officer (DPO) who will advise our organisation on the obligations required to comply with the GDPR and other data protection laws. The DPO will monitor compliance by managing internal data protection activities and advising on data protection impact assessments. The DPO will also train staff and conduct internal audits. This individual will be the first point of contact for the supervisory authorities and individuals whose data is processed.

Our firm ensures that it only appoints individuals who are capable and competent –

We will have a strict recruitment policy in place to ensure that the Data Protection Officer or person responsible for data protection has sufficient training or experience to carry out the role. We consider the candidate's skills, knowledge and experience whilst also ensuring that previous employment histories have been verified. This also ensures that individuals are only considered as candidates if they have enough time to satisfy relevant requirements.

The firm only appoints individuals after assessing their financial soundness –

We will ensure, the honesty, integrity and reputation questionnaire is implemented and includes questions around judgement, debts and bankruptcy proceedings. We will ensure all candidates answer each question and sign to acknowledge their answers are truthful. Additionally, the firm conducts credit history checks on proposed individuals prior to appointment. These measures ensure that individuals are only appointed after verification of their suitability.

The firm will ensure safe data usage and reduce the risk of improper data handling –

We ensure a regulatory risk assessment is in place to identify and assess the risk of improper data handling. We have assessed our use of personal data and identified areas where there are risks of regulatory breaches. Each risk has been allocated an impact score based on the nature and seriousness of the risk were it to materialise. We have set out our strategy by which we aim to mitigate and manage each risk.

We will implement procedures to ensure notification and disclosure of significant information/material to the ICO on matters of serious regulatory impact or on any change to the firm's core information –

After identifying the risk that the ICO may be unable to conduct its supervisory role sufficiently or that the ICO takes regulatory action against the firm, this will be discussed during the firm's management meetings. We will undertake discussions in relation to business information, we then collect, and report to the ICO any serious breaches. We will ensure the breach is reported to the ICO within 72 hours of becoming aware of it. To prevent reoccurrence of such breach, we will schedule regular management meetings to discuss any breaches, and to provide solutions to mitigate these in the future. Management team will take minutes of these meetings, as they will act as an accountability tool, record any issues discussed and decisions made concerning these issues.

We will ensure sufficient monitoring is in place to satisfy all regulatory requirements –

We will undertake an annual regulatory risk assessment to document our data use which is reviewed and updated on an annual basis, with appropriate remedial action carried out.

3. MANAGEMENT INFORMATION

To ensure our ongoing compliance with the regulations, we have endeavoured to ensure that management information is properly and comprehensively available to assist the senior management to monitor and asses the firm's actions regarding our regulatory requirements.

We have in place adequate systems and controls to monitor and ensure the overall compliance of the firm. In addition to this utilised Compliance Manual which contains extensive policies and procedures in relation to the regulated activities, an individual has been appointed with the responsibility to oversee the firm's compliance. That individual monitors and then reports to the board on a monthly basis. The reports form part of the board's management meeting agenda, informing the board of any issues and giving opportunity to discuss the measures required to ensure ongoing compliance.

We ensure that management information is gathered properly through a system that is in place which details what information is required, when it is required and for whom it is required. That information is then included in management meeting agendas, the minutes of which are recorded and stored. The data which is gathered includes:

- Complaints;
- Product Data;
- File Audits;
- Records of business transactions;
- Records of Internal Organisation;
- SAR Requests;
- Report listing any 'Personal Data Breaches';
- Breach Report Reviews; and

We also review Client Files monthly to ensure that client records are kept up to date.

Management Information will enable management to make informed business decisions. It is important that we ensure the management information is:

- Accurate - the correct numbers with any commentary contributed by the right people;
- Timely - sufficiently available to enable managers to act;
- Relevant - displaying what a manager can directly influence or something that they may need to escalate to facilitate the necessary action; and
- Consistent - consistent on a period-to-period basis to allow managers to spot trends and make sound decisions.

3.1 DEALINGS WITH THE FIRM

We operate key principles to ensure we are complaint with the regulations at all times:

- Clear reporting lines;
- Documented and appropriately apportioned responsibilities;
- Established systems and procedures for the identification and rectification of potential breaches of compliance;
- Clear methods for gathering and utilising management information; and
- Procedures for ensuring business continuity.

3.2 COMPLAINTS PROCEDURE

Our firm aims to ensure compliance by appropriate handling of any complaints received, dealing with those complaints in the appropriate manner and taking from each complaint, information relevant to ensuring that potential breaches are identifies and appropriately remedied.

4. DATA RECORDS POLICY

Regulatory requirements require firms to maintain appropriate records and audit trails to evidence compliance to the requirements, to demonstrate decision-making and to effectively investigate customer complaints. This Recording Policy sets out principles that we follow to ensure that we maintain adequate records and audit trails of our business conduct.

- We will record and store telephone calls to consumers for a period of no more than 3 years;
- We will record and store all written communications with clients including provision of information and correspondence and notes of conversations;
- We will record and store written communications with third parties;
- We will record and store all documentation pertaining to a client's file (i.e. product documentation, bank statements, terms and conditions and letters of authority;
- We will record and store completed due diligence documentation and relevant agreements with third parties;
- Where we have received consent to contact the customer we will keep evidence of consent;
- We will maintain records of staff training, monitoring and assessments;
- We will maintain records of contact with vulnerable customers;
- We will maintain records of complaints (i.e. subject matter of the complaint, details of the complainant, details of investigation carried out, outcome of the complaint, root cause analysis); and
- We will maintain records of compliance monitoring carried out.

4.1 DATA PROTECTION POLICY AND PROCEDURE

Our activity involves the collection of personal data and may involve the collection of sensitive personal data.

Data for the purposes of our products and services includes:

- Customer personal information;
- Customer transactional data; and
- Customer product data.

We only store and processes data in accordance with the data protection principles contained in the Data Protection Act 1998, and also, in line with the General Data Protection Regulation which came into force on 25th May 2018.

We have not identified any aspect of our products and services which breaches, or is likely to breach, the requirements of the Data Protection Act 1998.

Data is retained in connection with our products and services for a period of six years in the case of customers and three months in the case of data subjects who have engaged with us but have not become customers. If we are unable for any reason to provide an exact timescale for data retention of particular information, we will provide a framework of the criteria used to determine this period.

The Information Commissioner enforces the Data Protection Act 1998, and the General Data Protection Regulation; which give individuals the right to know what information is held about them, and provides the framework to ensure that personal information is handled correctly.

Our legal responsibilities under the Act are:

- To notify the Information Commissioner Office that we are processing information;
- To process the personal information in accordance with the eight principles of the Act; and
- To answer subject access requests received from individuals;

Responsibility for overseeing Data Protection includes:

- Ensuring that the Information Commissioner is notified, and that the notification is kept up to date. Renewal of the Firm's registration costs an annual fee, no VAT charge and is payable to the Information Commissioner's Office;
- Ensuring that the people whose information we hold, know that we have it, and that they are likely to understand what it will be used for;
- Ensuring that there are sufficient safety measures in place to protect personal information under the Data Protection Act 1998 which are appropriate for the different records held whether they are on paper or digitally;
- Ensuring that access to personal information is limited to those on a strictly need to know basis;
- Ensuring that personal information is accurate and up to date;
- Ensuring that personal information is deleted or destroyed as soon as there is no further need for it;

- Ensuring that all employees are trained in their duties and responsibilities under the Data Protection Act, and assess whether they are putting them into practice;
- Ensuring that any notice of breach is reported to the Information Commissioner's Office within 72 hours;
- Ensuring that all personnel are made aware that Exemption 29 under the Data Protection Act can be applied if the police need some information for the prevention and detection of crime or for the apprehension or prosecution of offenders. This exemption cannot be used by the police as a 'fishing exercise', which means that they cannot ask for all records in the hope of catching offenders but must have a specific request and a need for this information. Only if we are satisfied that the information is going to be used for this purpose and they have given a specific reason for wanting this information can the information be disclosed;
- Ensuring that if we have a legitimate reason for recording calls e.g. for staff training purposes that people are made aware of this;
- For being aware that the Act provides individuals with important rights, including the right to find out what personal information is held on electronic and most paper records;
- For being aware that should an individual or organisation feel they're being denied access to personal information they are entitled to, or feel their information has not been handled according to the eight principles, that they can ask the Information Commissioner to help;
- Ensuring that third party information is removed from computer records before being disclosed;
- Ensuring that manual records which are contained within a ''relevant filing system'' are disclosed on request and that the files which form part of the relevant filing system are structured or referenced in such a way that information about the applicant can be easily located. Where manual files fall within the definition of a relevant filing system, the content will either be sub-divided, which allows the searcher to go straight to the correct category and retrieve the information requested without a manual search, or will be indexed to allow the searcher to go directly to a relevant page(s); and
- Drawing up a Data Security Policy based on the above which is specific to us and ensure that senior management communicate this to everyone within our company. Please refer to our Data Security Policy below.

Everyone within the Firm who processes personal information must comply with the eight principles, which make sure that personal information is:

- Fairly and lawfully processed;
- Processed for limited and specifically stated purposes;
- Used in a way that is adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary;
- Processed in line with individuals' rights;
- Kept safe and secure; and
- Not transferred to other countries without adequate protection.

There is stronger legal protection for more sensitive information which relates to information including:

- ethnic background;
- political opinions;
- religious beliefs;
- health;
- sexual health; and
- criminal records.

Those who process personal information must also:

- Inform the person within the firm who is responsible for Data Protection if a subject access request is made by an individual using their right under the Data Protection Act;
- Ensure that customers are given Customer Documentation which outlines what and how their information is going to be processed. This is to make sure the individual knows exactly what is going to happen to their information and how it is going to be used;
- Not do anything with personal information unless the individual is made aware;
- If a person enquires or wishes to make changes to another customer's agreement you must ask them to ask the customer to send written authorisation showing that they may act for them; and
- Ensure that compliance activities are regularly reviewed to ensure adequate resource and support is being given to these activities.

4.2 CLIENT COMMUNICATION

We communicate with the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Our firm supports the notion of accountability and transparency that are introduced by the General Data Protection Regulation. We will always endeavour to engage our clients with truthfulness and provide full information where we are able to do so. It is our clients who drive the success of our business, and we will handle all personal data with the upmost integrity.

4.3 STAFF CONDUCT

We will ensure that it is clear to workers the circumstances in which they may or may not use the employer's telephone systems (including mobile phones), the e-mail system and internet access for private communications under the employment practices code.

In compliance with the employment practices code, we will ensure that all workers are aware how they can be criminally liable if they knowingly or recklessly disclose personal information outside their employer's policies and procedures.

We are aware that workers as well as employers have responsibilities for data protection under the Act. Line managers have responsibility for the type of personal information they collect and how they use it. No-one at any level should disclose personal information outside the organisation's

procedures, or use personal information held on others for their own purposes. Anyone disclosing personal information without the authority of the organisation may commit a criminal offence

The new accountability principle in Article 5(2) requires demonstrating that the firm will comply with the principles and states explicitly that this is the firm's responsibility. The effect of the overarching principle for accountability means that our firm must embed a regime for the protection of data throughout all of our processes and, where necessary, implement appropriate technical and organisational measures that ensure and demonstrate that continuous compliance. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies. We must also make sure that we maintain relevant documentation on our processing activities, so as to ensure we sustain an effective audit trail.

We seek to ensure that all staff are aware of their individual roles and obligations under the Data Protection Act 1998, and the upcoming General Data Protection Regulation. Our senior management ensure to arrange periodic training in respect to the importance of data protection within our firm, specifically we seek to arrange frequent pre-emptive training in respect to the specific effects that the General Data Protection Act will have in relation to our firm. We monitor training, and provider refresher training on a scheduled basis. Our senior management will keep up to date with any regulator updates and changes within our industry,

We ask for all staff to secure their computer (or log off when not at their desk) and to never give out their individual password; we make it clear to all staff members that they are responsible for whatever action is taken through their account, whether their conduct or another's. We have a strict phones policy, and integrate DPA checks on all calls, where personal information is to be given out. We express a need for cautiousness and diligence in respect to correspondence in any form.

- We instruct all staff to shred confidential waste, and only to send documentation when ready to collect from the tray; and
- We operate a clean desk policy. All files are to be put away in cabinets at the end of each day, along with any other relevant documents that may contain sensitive data.

5. DATA PROCESSING POLICY AND PROCEDURE

Our firm ensure that wherever we engage in data processing we adhere to, and are compliant with, the Data Protection Act 1998 (DPA). From the 28th of May 2018, many of the provisions of the DPA will be revised and replaced by the succeeding GDPR. We are aware that the GDPR brings practical changes to data processing and have organised out internal data processing systems to adhere to the regulations requirements. In all circumstances where we undertake the processing of data, we always ensure that:

- The data subject has given his or her consent to the processing; and
- That the processing is necessary:
- For the performance of a contract to which the data subject is a part; or
- For the taking of steps at the request of the data subject with a view to entering into a contract.
- The processing is necessary for compliance with any legal obligation which the data control is subject, other than an obligation imposed by contract.

- The processing is necessary to protect the vital interest of data subject.
- The processing is necessary:
    - For the administration of justice;
    - For the exercise of any functions conferred on any person by or under any enactment;
    - For the exercise of any functions of the Crown, a Minister of the Crown or a government department; or
    - For the exercise of any other functions of a public nature exercised in the public interest by any person.
- The processing is necessary for the purposes of legitimate interests by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
    - The Secretary of State may, by order, specify circumstances in which this condition is, or is not, to be taken to be satisfied.

A legitimate interest, in respect to the processing of data can be defined as:

- Lawful, compliant with relevant laws (especially the laws of individual member states when engaged in the processing of international data);
- Be sufficiently clearly and articulated to allow a balance test (to review the balance of the legitimate interest against the wishes of the data subject) to be carried out; and
- Represent a real and present interest that is not merely a speculative interest.

5.1 PROCEDURE FOR PROCESSING PERSONAL INFORMATION

Everyone within the Firm who processes personal information must comply with the eight principles making sure personal information is:

- Dealt with Fairly and lawfully processed;
- Processed for limited and specifically stated purposes;
- Used in a way that is adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary;
- Processed in line with individual's rights;
- Kept safe and secure; and
- Not transferred to other countries without adequate protection.

We will meet these obligations by:

- Ensuring all data is kept safely and securely wither on password protected devices or locked up in lockable or password protected cupboards;
- Ensuring there is a record of the date the data was captured and where possible monitor the timeframe by checking regularly if we are still required to hold the data;
- Ensuring any changes or updates are recorded as soon as they are given to the firm by the individual; and
- Ensuring there are no restrictions placed on the data by the individual.

There is stronger legal protection for more sensitive information, such as:

- ethnic background;
- political opinions;
- religious beliefs;
- health;
- sexual health; and
- criminal records.

Those who process personal information must also:

- Inform the person within the firm who is responsible for Data Protection if a subject access request is made by an individual using their right under the Data Protection Act;
- Ensure that customers are given Customer Documentation which outlines what and how their information is going to be processed. This is to make sure the individual knows exactly what is going to happen to their information and how it is going to be used;
- Not do anything with personal information unless the individual is made aware;
- If a person enquires or wishes to make changes to another customer's agreement you must ask them to ask the customer to send written authorisation showing that they may act for them; and
- Ensure that compliance activities are regularly reviewed to ensure adequate resource and support is being given to these activities.

6. INFORMATION NOTICES POLICY AND PROCEDURE

Controllers most provide information notices to ensure the transparency of processing. The Information Commissioner's Office specifies a set list of information that must be provided. We are aware that the following must be provided by us at the time new data is obtained. If a controller does not obtain the information directly, then this must be provided within a reasonable period of having obtained the data, or at a maximum of one month.

- [If applicable] the contact details of the data protection officer
- Legal basis for processing – including the legitimate interest pursued by the controller (or third party) if there is a legal basis.
- Details of any transfers outside the EU
    - Including how the data will be protected (e.g. the recipient is in an adequate country; Binding Corporate Rules (BCR) are in place etc.); and
    - Details of how the individual can obtain a copy of the BCRs
- The retention period for the date – if not possible, then the criteria used to set this.
- That the individual has a right to access and port data, to rectify, erase and restrict his or her own personal data, to object to processing and, if processing is based on consent, to withdraw consent.
- That an individual can complain to a supervisory authority (e.g. ICO)
- Whether there is a statutory or contractual requirement to provide the data, and the consequences of not providing the data.

6.1. INFORMATION NOTICE - PRIVACY POLICY

Any reference to “we” or “us” in this privacy policy shall mean Victoria Mutual Finance Limited. This privacy policy applies to this website which is owned and operated by Victoria Mutual Finance Limited.

Throughout this privacy policy “you” means the customer.

We believe you deserve the utmost respect when it comes to the security and use of your personal information, so we have described how we look after your information as clearly as possible.

Leighton Smith is our data protection officer and is responsible for the way our firm handles personal data.

INFORMATION WE COLLECT

We collect information about you in which you provide to us through our website and through communications with us.

In addition to the personal and financial information you submit (or we collect), we may collect information about your computing including, where available, your IP address, operating system and browser type.

We may also record and/or monitor calls for quality checks and staff training.

INFORMATION WE HOLD

We will hold information about you including: name, address, phone numbers, email address, date of birth, employment and banking and financial details.

We will also hold information about you from when you contact us and when we contact you.

Any other information which we reasonably need to operate your account or fulfil our regulatory obligations will also be held by us.

HOW WE WILL USE INFORMATION ABOUT YOU

Subject to having obtained specific consent under Article 4 of the General Data Protection Regulation. We will use your information to help identify, develop or improve products that may be of interest to you. We will contact you by email, SMS, letter, telephone or in any other way about our products and services, unless you tell us that you prefer not to receive marketing.

The information will be used to enable us to monitor and analyse our business and carry out market research. This information may be provided to independent external bodies such as governmental departments and agencies only when requested by law.

Your data may also be used for other purposes for which you give your permission or where we are permitted to do so by law or it is in the public interest to disclose the information or is otherwise permitted under the terms of the General Data Protection Regulation and the Data Protection Act 1998.

YOUR RIGHT TO CANCEL TO DIRECT MARKETNG

You have the right to object to direct marketing. Please inform us of your objection by either calling us at 0207-738-6799, or email at manager@myvmgroup.com

INFORMATION WE SHARE

We will keep your personal information confidential and only share it with others for the purposes explained in this policy.

We will not under any circumstances sell or share your data with third party marketing companies. We may however share the following information about you:

- Within Victoria Mutual Finance Limited and office locations in the United Kingdom;
- With any mortgage intermediary system we may use;
- With any payment system we may use;
- With regulatory and governmental authorities' ombudsmen, or other authorities, including tax authorities, including those overseas, where we are requested by them to do so.

ACCESS TO YOUR OWN INFORMATION

You have the right to request a copy of the information which we hold about you. This is called a Data Subject Access Request, which you can make by writing to Donna Brown at 380 Brixton Road, SW9 7AW.

We may charge an administrative fee when a request is manifestly unfounded or repetitive. We may also charge a further administrative fee when you request for us to provide further copies of the information already provided to you.

We want to make sure that your personal information is accurate and up to date. You may ask us to correct or remove information you think is inaccurate. We will respond to your request within one month of receiving your request. We will inform you of the third parties to whom your data has been disclosed.

YOUR RIGHT TO WITHDRAW CONSENT

You have the right to withdraw your consent at any time. You can do so by emailing us at manager@myvmgroup.com or writing to us at Victoria Mutual Finance Limited, 380 Brixton Road, SW9 7AW.

RIGHT TO MAKE A COMPLAINT TO A SUPERVISORY ADVISOR

You have the right to make a complaint to a supervisory authority. Please do so by contacting Leighton Smith at 0207-738-6799 | Leighton.smith@myvmgroup.com|380 Brixton Road, London SW9 7AW.

TRANSFER OF INFORMATION

We may transfer your personal information abroad to other countries outside of the UK. If we do so, we will ensure the information is held securely to standards at least as good as those in the UK and only used for the purposes set out in this privacy policy.

THIRD PARTY LINKS

Our website contain links to third party websites of other companies within the Victoria Mutual Group. If you follow a link to any of these websites, please note that these websites maintain similar terms and privacy policies.

CHANGES TO OUR PRIVACY POLICY

We keep our privacy policy under regular review, and we will place any updates on this webpage www.vmfinanceltd.com. This privacy policy was last updated on January 22, 2021.

CONTACTING US

You can contact us at:

Main Address:
380 Brixton Road
SW9 7AW

Telephone:
Brixton: 0207-738-6799
Tottenham: 0208-801-6777
Birmingham: 0121-454-2020

Email:
manager@myvmgroup.com

7. SUBJECT ACCESS REQUEST POLICY

Our firm must provide a copy of some personal data undergoing processing, commonly known as a subject access request ('SAR'), when requested. In clear terms, a subject access enables an individual to find out what personal data our firm holds about them. This must be provided free of charge initially, however, in the event that any further copies are requested, we may charge a reasonable, administrative cost-fee. In this context, excessive or identical requests for a data subject's data are chargeable, as far as is reasonable for the cost our firm incurs. Our firm must ensure that where the request is made in an electronic form, the subject must receive the requested information in an accessible and commonly used electronic form.

In compliance to Recital 63 of the GDPR, we will endeavour (where possible) to provide a secure system that will grant the data subject direct access to his/her data, however, it must be duly noted that this is not a strict obligation.

Within the requested SAR, we will include:

- The purpose of processing;
- The categories of data processed;
- The recipients, or categories of recipients (in particular, details of disclosure to recipients in third countries or to international organisations).

- Our complaints escalation process

In addition to the above, we will include where practicable:

- The envisaged retention period [of the data], or if this is not possible, the criteria used to determine this period;
- The individual's rights of rectification or erasure, to restrict processing or to object to processing and to lodge a complaint to a supervisory authority;
- Information regarding the source of the data (if not collected from the data subject); and
- Any regulated automated decision taking (i.e. decisions taken solely on an automated basis and having legal or similar effects; also, automated decision taking involving sensitive data) – including information about the logic involved and the significance and envisaged consequences of the processing for the data subject.

In the event that we do not comply with a SAR, we will provide reasons for not doing so.

We note that the data subject's right to access to personal data, should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. Where a processor such as ourselves processes a large quantity of information concerning the data subject, we will request that, before any information is delivered, the data subject specify the information or processing activities to which the request relates.

8. DATA RECTIFICATION POLICY

As a firm holding a large quantity of data, we are entitled to write counter-correspondence to request that the data subject specifies the information or processing activities to which the request relates.

On receiving the above information, if a data subject recognises any information we hold at the time of the request to be inaccurate, then we will adhere to a request, as controller of the information, to rectify any inaccuracies identified. Furthermore, where a data subject makes it known that their personal data is incomplete, we will acknowledge and act on any request to complete the data, or in lieu provide a supplementary statement. A supplementary statement would advise on the data currently being held, and if the data could not be immediately acted upon, this document would advise on the course of action to be taken by the firm.

9. DATA PORTABILITY POLICY

In respect of our obligations under the General Data Protection Regulation, our firm will adhere to the guidance on data portability, and ensure that any information provided in response to a SAR, is structured in a '…commonly used and machine readable form'. We are aware that, if requested by a data subject, we may be required to transmit such data directly to another data controller.

This will only apply to:

- Personal data which is processed by automated means (no paper records)
- Personal data which the data subject has provided to the controller, which formed part of the information collated throughout the data subject and the controller's engagement; and
- Where additional data has been obtained under the belief that it was necessary at the time;
- Only where the basis for processing is consent, or that the data are being processed to fulfil a contract or steps preparatory to a contract.

10. THE RIGHT TO ERASURE POLICY AND PROCEDURE

Individuals can require data to be 'erased' when there is a problem with the underlying legality of the processing or where they withdraw consent. An individual can require the controller to restrict processing of the data whilst complaints are resolved, or if the processing is unlawful but the individual objects to erasure. Instances in which this may be the case are: where the data subject wishes for the data controller to maintain his information on records, for the purpose of pursuing a legal claim, or; where the data subject may be required by another authority, such as the police forces, to maintain the information for the purpose of assisting with a criminal investigation.

As a controller, the right to erasure or 'to be forgotten', will apply:

- When data are no longer necessary for the purpose for which they were collected or processed;
- If the individual withdraws consent to processing (and if there is no other justification for processing);
- To processing based on legitimate interests- if the individual objects and the controller cannot demonstrate that there are overriding legitimate grounds for the processing;
- When the data are otherwise unlawfully processed;
- If the data has to be erased in order to comply with Union or Member State law which applies to our firm.

The right to be forgotten is enshrined in Article 17 of the General Data Protection Regulation, and requires firms to weigh data subjects' rights against any competing rights and interests. The right to erasure should also be extended in such a way that a controller who has made the personal data public online should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, a controller should take reasonable steps, taking into account available technology and the means available to him, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

The right to restriction of processing within Article 18 of the General Data Protection Regulation, essentially replaced the provisions in the Data Protection Directive on 'blocking. In some situations, this right will give an individual an alternative to being erased in an absolute and definite way. If personal data is 'restricted', then the controller may only store the data. In the circumstance, the controller will not be permitted to further process the data unless:

- The individual consents; or
- The processing is necessary for establishment etc. of legal claims;
    - for the protection of the rights of another natural or legal person;

- for the protection of important (Union or Member State) public interest.

If it is the case that the data has been disclosed to others, then the controller must notify these recipients about the restricted processing, unless this would require a disproportionate effort, or is impossible in the circumstances (General Data Protection Regulation, Article 62).

In respect of the methods our firm will use in order to restrict the processing of personal data, we will, for example:

- Temporarily move the selected data to another processing system
- Make selected personal data unavailable to users
- Temporarily remove any published data from our website

There are six categories for exemption in respect to the right of erasure. The obligation to erase data does not apply if processing is necessary for:

- For the exercise of the right of freedom of expression and information;
- For compliance with a Union or Member State legal obligation;
- For performance of a public interest task or exercise of official authority;
- For public health reasons;
- For archival, research or statistical purposes (if any relevant conditions for this type are met); or
- If required for the establishment, exercise or defence of legal claims.

11. PRIVACY BY DESIGN – POLICY AND PROCEDURE

Organisations must implement technical and organisational measures to show that they have considered and integrated data compliance measures into their data processing activities, specifically this relates to the adaptation of appropriate staff policies and the use of pseudonymisaton.

Pseudonymisaton is a privacy enhancing technique where information which allows data to be attributed to a specific person and to be held separately and subject to technical and organisational measures to ensure non-attribution to specific data subjects without the use of additional information. By technical and organisational measures, this just refers to the specifics of our firm and what technical instruments we have at our disposal, this may take into consideration the existence of third party

Our firm is committed to ensuring that all data related risks are mitigated to their most capable extent. Our firm will seek to implement technical and organisational measures, in order to demonstrate and integrate data compliance measures into our data processing activities. We organise all of our conducted business in such a way which builds on the idea of privacy by design, such as the provision of training to all staff members so they have a sufficient awareness of data protection, and our firm's processes to maintain this. We will put into place sufficient systems and controls which serve to

To ensure the above, our firm uses data-masking, to protect confidential information that directly or indirectly reveals an individual's identity. For the purpose of clarity, data masking is a method of creating a structurally similar but inauthentic version of an organisation's data that can be used for purposes such as software testing and user training. The purpose is to protect the actual data while having a functional substitute for occasions when the real data is not required.

12. PRIVACY IMPACT ASSESSMENTS POLICY AND PROCEDURE

As a firm handling personal data, we are required by the General Data Protection Regulation to implement a wide range of measures to reduce the risk of any breach. One of the most significant actions we must take is to produce a Privacy Impact Assessment ('PIA'). A PIA should be created when our firm is looking to start a new project or is deciding upon an action which may have the propensity to effect an individual's privacy rights.

A PIA is an assessment to identify and minimise non-compliance risks. Specifically, our firm must ensure that a PIA has been run on any "high risk" processing activity before it is commenced (this is measured by reference to the risk of infringing a natural person's rights and freedoms).

Our firm will ensure that all PIAs we produce include:

- A description: of the processing activities and their purpose;
- An assessment of the need for and proportionality of the processing, the risks arising and measures adopted to mitigate those risk, in particular safeguards and security measures to protect personal data and comply with the GDPR.

A supervisory authority must be consulted *before* any data processing commences if a PIA identifies a high unmitigated risk. If it is necessary in the circumstance, we will seek the views of affected data subjects "or their representatives" in conducting a PIA, if appropriate.

Our firm follow a routine procedure in the production of any PIA; our procedure takes place as follows:

1. Identifying the need for the PIA

The need for a PIA can be identified as part of our usual project management process,

2. Describing the information flows

Describe the information flows of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information.

3. Identifying the privacy and related risks

Some will be risks to individuals – for example – damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy,

Some risks will be to our firm, for example damage to reputation, or the financial costs or a data breach.

Legal compliance risks include the DPA, PECR, and the Human Rights Act 1998.

4. Identifying and evaluating privacy solutions

We will explain how we could address each risk concerned. Some might be eliminated altogether, whilst others may only be reduced. Most projects will require use to accept some level of risk, and will have some impact on privacy.

We will evaluate the likely costs and benefits of each approach. We will think about the available resources, and the need to deliver a project which is still effective.

5. Signing off and recording the PIA outcomes.

Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of our wider project approval.

Our PIA report will summarise the process, and the steps taken to reduce the risks to privacy. It will also record the decisions taken to eliminate, mitigate, or accept the identified risks.

By publishing a PIA report, our firm will be able to improve its transparency and accountability, and will let data subjects learn more about how our project may affect them.

6. Integrating the PIA outcomes back into the project plan

Our PIA findings and actions should be integrated with the project plan. It might be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

Our PIA might generate actions which will continue after the assessment has finished, and so in accordance, we will revisit the PIA to ensure that these are monitored.

We will also record what we learn from the PIA for the purpose of future projects.

13. BREACH REPORTING POLICY AND PROCEDURE

Personal data and breaches and notification

Under the General Data Protection Regulation, ('GDPR'), all breaches will have to be reported. Although this obligation applies with the incurrence of a breach of any level of severity, particular attention must be paid by a firm to those breaches which are likely to result in a high risk to the rights and freedoms of individuals.

For the purpose of clarity, a 'high risk' means the threshold for notifying individuals is higher than for notifying the Information Commissioner's Office; a notification must be made directly and immediately. High risk may result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

In case of an incident defined as, "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed", the new breach notification regime under the GDPR will apply as follows:

1. *Obligation for data processors to notify data controllers*

Timing:

Without undue delay after becoming aware of it.

Exemption:

None in the GDPR

Observations:

- All breaches will have to be reported.
- EDPB to issue guidelines to clarify the notion of "undue delay" and the particular circumstances in which a data processor is required to notify the personal data breach.

2. *Obligation for data controllers to notify the supervisory authority*

Timing:

Without undue delay and, where feasible, not later than 72 hours after becoming aware of it.

Exemption:

No reporting if the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Observations:

- When the timing obligation is not met, reasons will have to be provided to the supervisory authority (e.g. request from a law enforcement authority).
- EDPB to issue guidelines to clarify the notion of "undue delay" and the particular circumstances in which a data controller is required to notify the personal data breach.

3. Obligation for data controller to communicate a personal data breach to data subjects

If the data controller is yet to do so, the supervisory authority may compel the data controller to communicate a personal data breach with affected data subjects unless one of the three exemptions is satisfied.

Timing:

Without undue delay: the need to mitigate an immediate risk of damage would call for a prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for communication.

Exemption:

No reporting is required if:

- The breach is unlikely to result in a high risk for the rights and freedoms of data subjects and this can be demonstrated. For example, the data may have been rendered unintelligible through encryption. Please see the regulatory risk assessment for more detail;
- Appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); or
- This would trigger disproportionate efforts (instead a public information campaign or "similar measures" should be relied on so that affected individuals can be effectively informed)

Documentation requirements in relation to breach reporting

In respect to our duties under the General Data Protection Regulation, our firm will ensure that it maintains:

- An internal breach register: this is an obligation for the data controller (our firm) to document each breach incident "comprising the facts relating to the personal data breach, its effects and the remedial action taken". The supervisory authority may be requested to assess how data controllers comply with their data breach notification obligations.

- There are also prescribed requirements to satisfy in the communication to the supervisory authority, e.g.
  - Describing the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned, etc.

- The communication to affected individuals e.g.

- Describe in clear and plain language the nature of the personal data breach and provide at least the following information:

  (i) the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
  (ii) the likely consequences of the personal data breach; and
  (iii) the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects).

Failure to meet the above requirements exposes the organisation to an administrative fine of up to €10,000,000 or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In general, the GDPR establishes a tiered approach to penalties for breach which enables the DPA's to impose fines for some infringements of up to the higher of 4% of annual worldwide turnover and €20,000,000. Other specified infringements would attract a fine of up to the higher of 2% of annual worldwide turnover and €10,000,000. A list of points to consider when imposing fines (such as the nature, gravity and duration of the infringement) is included.

These percentages apply to an 'undertaking' and a last-minute clarification in the Recitals adds that this is defined in Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU).

14. DATA SECURITY BREACH REGISTER

We will keep records of all personal data breaches in an inventory or log.

It must contain at minimum:

- the facts surrounding the breach;
- the effects of the breach; and
- remedial action taken

In the event of any data security breach, we will always aim to submit as much information as possible, for both the benefit of the Regulator and for our own benefit so as to mitigate the risk of any reoccurrence of the breach.

Wherever a data security breach occurs we will document all available information so that the information can be presented to the regulator within the required timeframe of 72 hours following the occurrence of that breach. We will also use this information to mitigate against the risk of any reoccurrence of the breach. That information will include:

- Firm's name
- Date of breach
- No people affected
- Nature of breach (choose most relevant)

- Description of breach
- How you became aware of breach
- Description of data
- Consequences of breach
- All individuals informed
- Remedial action
- Other Regulators informed
- When did you first notify the ICO of the breach?

[Name] must also submit this log in a form format set (available on ICO's website) to ICO, on a monthly basis.

15. PERSONAL DATA BREACH REGISTER

A personal data breach may mean that someone other than the data controller (our firm) gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within an organisation, or if a data controller's own employee accidentally alters or deletes personal data. In the event of a breach we will notify the Information Commission's Office ('ICO') within 24 hours of becoming aware of the essential facts of the breach. Our notification to the ICO will include as a minimum:

- Our name and contact details;
- The date and time of the breach (or an estimate);
- The date and time we detected it;
- Basic information about the type of breach; and
- Basic information about the personal data concerned.

We are aware that a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

16. DATA SECURITY POLICY AND PROCEDURE

The main purpose of this data security policy and procedure is to inform staff and managers of the obligatory requirements for protecting technology and data. Data is an information asset to the business and thus should be protected. This policy specifies the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit our internal systems and processes for compliance with the policy.

In line with Article 26 (Recital 78) our firm must ensure that we implement appropriate technical and organisational measures to be taken to ensure that the requirements of the General Data Protection Regulation are met. In order to be able to demonstrate compliance with the Regulation, we must adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

Under the General Data Protection Act, we are required to ensure a clear allocation of our all staff's responsibilities. We ensure that we are able to demonstrate compliance by maintaining extensive records of all processing activities under our responsibilities. We ensure that we are able to cooperate with the Information Commissioner's Office, and on request make our records available, so that they may serve for monitoring our processing operations.

[Name] will be responsible for implementation and oversight of this policy, and will conduct a review on a quarterly basis.

Legislative Background

Data security is governed by the General Data Protection Regulation, and the Data Protection Act (DPA) 1998, under which Principle 7 declares:

Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected.

The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle—

(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

(b) take reasonable steps to ensure compliance with those measures.

Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless—

(a) the processing is carried out under a contract—

(i) which is made or evidenced in writing, and

(ii) under which the data processor is to act only on instructions from the data controller, and

(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

To summarise, the DPA requires every firm to have appropriate security to prevent the personal information of our clients being accidently or deliberately compromised.

What Needs Protecting?

The key assets which require protection are:

- Hardware: CPUs, boards, keyboards, terminals, workstations, personal computers, laptops, other portable devices, printers, disk drives, communication lines, terminal servers, routers.
- Software: source programs, object programs, utilities, diagnostic programs, operating systems, communication programs.
- Data: during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media.
- People: users, administrators, hardware maintainers.
- Documentation: on programs, hardware, systems, local administrative procedures.
- Supplies: paper, forms.

Each type of data may be categorised within three categories: Physical Security, IT Security and Intellectual Property.

Management and organisational measures

It is important to identify a person or department in your organisation with day-to-day responsibility for security measures. They should have the necessary authority and resources to fulfil this responsibility effectively. The person within our firm responsible for oversight of data security is [name], who will conduct a review of this policy on a quarterly basis.

Physical Security

The building is protected from unauthorised access by:

- Burglar Alarm and Automated Shutters
- Bullet proof office front glass
- Locked internal door with fob key access, preventing access to main office area
- Security cameras
- Staffed reception area to vet and sign in visitors.

Protecting Documents in the Office

Documents are protected from unauthorised access by:

- Locked cabinet for storage of all paper documents;
- Locked, fireproof safe for overnight storage of important client documents or cheques;
- A clear desk policy is in place to avoid documents left on desks and on view overnight;
- Confidential paperwork is placed in secure containers and shredded weekly; and
- All documents are scanned and shredded within one day of receipt**. Use of External Third Parties/ Outsourcing**

If any IT administration processes such as back up of data, support of the various IT systems and data storage are outsourced the specific procedures will be followed and due diligence on the firms concerned carried out.

Other third parties e.g. cleaners or cleaning companies whose staff can access client data will also be subject to the same due diligence.

Our procedures will include:

- Understanding the third party's data security procedures
- Carrying out appropriate due diligence on those third parties, including their data security arrangements and staff recruitment policies
- Considering whether we should allow third parties unsupervised access to the office or records.

IT Security

These are the means by which we ensure that any information stored electronically is kept secure from unauthorised access.

Protecting Infrastructure and Hardware

We use computer safeguards such as firewalls and data encryption, we enforce physical access controls to our buildings and files, and we only authorise access to those employees who require it to fulfil their job responsibilities. When you share data with us through the website, that information is protected by secure socket layer (SSL) encryption. This link ensures that all data passed between the web server and browsers remain private and integral. Our security systems meet industry standards and we are constantly monitoring internet developments to ensure our systems evolve as required.

Use of Personal Devices

Staff may use personal devices for work in circumstances where the firm is experiencing internal hardware issues, but only where this has been agreed in advance and the following points have been considered:

- Being clear with staff about which types of personal data may be processed on personal devices and which may not.
- Using a strong password to secure their devices.
- Enabling encryption to store data on the device securely.
- Ensuring that access to the device is locked or data automatically deleted if an incorrect password is input too many times.
- Using public cloud-based sharing and public backup services, which you have not fully assessed, with extreme caution, if at all.
- Registering devices with a remote locate and wipe facility to maintain confidentiality of the data in the event of a loss or theft.

Disposal of Hardware

Consideration is given to the disposal of computers, laptops, other portable devices, memory sticks, disks etc.

- If a third party is used for the disposal of data, the firm will satisfy itself with their data security and staff vetting arrangements

- Disposal of a computer (or other equipment which potentially stores client records e.g. some photocopier/scanner equipment); the hard drive will be wiped with specialist software or removed and destroyed sufficiently so that information cannot be accessed by an authorised person.

Access Rights

Access rights to information on the network and emails are controlled through an Access Right Policy. This policy ensures that:

- Access is granted to data only where required and where approved by an authorised person;
- Temporary access to data must also be time bound, and privileges revoked after that date or an extension expressly granted by an authorised person;
- Network administration is subject to a credit check and Disclosure and Barring Service Check (previously CRB check) on appointment, in addition to full referencing etc.; and
- All staff who access client/sensitive information are subject to an annual vetting process (this could include credit checks and/or Disclosure and Barring Service checks).

A register is maintained listing what access rights have been given and to which staff. This is maintained and updated by [name].

Data Security Violations/ Data Compromise Reporting Policy

All staff are under an obligation to report any incident which they may feel violates the data security of the business by informing [name]. All violations are recorded in the Data Security Violations Register.

Equally all staff are aware of the need to report any data compromise incidents. These can include:

- Loss of laptop or other portable device;
- Loss of client data either in paper form or electronic;
- Loss of memory sticks/disks/USB pens etc.;
- Unauthorised persons in back office area where data stored; and
- Client information passed onto unauthorised third party.

All incidents should be reported immediately to [name] and these will be recorded on a Data Compromise Register. The firm's policy on this is for additional training to be provided to the staff involved and for the client concerned to be notified.

Audits

Compliance with this policy is audited on an annual basis by [name]. The results are detailed in the Security Audit Log.

Appendix 1 – Data Security Violations Register

Date Violation Identified	How Violation was Discovered	Date of Actual Violation	Description of Violation	Date of Notification to Regulator	Any Remedial Action

Appendix 2 – Data Security Audit Register

Date of Audit	Area Audited	Name of Auditor	Results of Audit	Any Remedial Action

17. DATA PROTECTION ASSESSMENT

This assessment must be completed by everyone on an annual basis, signed off by the person responsible for Training and Competence and stored in the individual's training file.

Name:

1. Who is responsible for Data Security?
2. In what circumstances could you release information to a customer's spouse?
3. You are copying a customer's proposal form, but the bottom of the form does not copy clearly so you copy it again. What do you do with the poor copy?
4. Within how many calendar days must we respond to a request by a data subject for access to the data we hold?
5. You call a customer to discuss their account. The phone rings and someone picks up and asks what the call is regarding. What do you tell them?
6. Where can you find details of VMFL's Data Protection Procedures?
7. What is the purpose of data protection?
8. It is the end of your shift. What do you do with the documents on your desk which contain customers' details?
9. The Information Commissioner's Office is responsible for enforcing data protection laws and regulations. True or false?
10. Can you disclose a customer's personal information to the police for the investigation of a crime? Yes or No?

Percentage correct:

Signed:..... (Manager)

Date:.....