Procedure for Data Protection

FCAP020

Objective:
To ensure that Data Protection obligations are met within our organisation.

Scope:
Throughout the whole organisation, including Suppliers and any person undertaking work on behalf of our organisation.

The person responsible for Data Protection is the (Director) referred to as "the nominated person".

All documents are approved by the nominated person for use and regularly checked and updated as and when required.

A monthly check is carried out through ICO and the ICO newsletters and updates by the nominated person to see if there are any changes in policies or documentation that requires action.

Corrections and changes are made whenever necessary and amended in the Master Document List on the computer. The version or issue number is changed and the previous version is placed in the archived folder. Obsolete documents are removed from the Master List and replaced with updated versions.

This procedure is issued to all Members of Staff including Sub-Contractors (if applicable), Sales Staff and Suppliers.

All documents and data are backed up separately at the end of each day and uploaded to a server at a separate location by the nominated person.

Foreword

It is a legal requirement under the Data Protection Act to ensure that personal information is properly protected. CONC 2.5 of the Consumer Credit sourcebook prohibits firms from unfairly passing customers' personal data – including payment details – to third parties, without consent or for a purpose other than that for which consent was given. This is also likely to breach the Data Protection Act.

Our firm must comply with the requirements of the Data Protection Act 1998 when processing personal data and that protecting personal information is a legal requirement under the Data Protection Act 1998.

All members of staff, including sales staff and suppliers must pay sufficient attention to the way personal information is handled and kept safe.

These policies and procedures are a response to these needs. They set out the steps that every individual should take to monitor, control and to mitigate the risk should personal information be lost or data protection systems fail.

The robust application of the guidelines coupled with the characteristic vigilance of staff will help to reduce the risks associated with handling personal data.

Introduction

This document sets out the protocols which govern our company's compliance with the Data Protection Act 1998.

Our firm will provide awareness sessions towards ensuring that all employees, sub-contractors and any person/s working on behalf of the company comply with the obligations under the Data Protection Act 1998.

Definitions

Personal Data
The Data Protection Act 1998 regulates the use of "personal data".

Personal data is data which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller.

Personal Data includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

Sensitive Personal Data

The following categories of data have been defined as 'sensitive personal data' under the Data Protection Act 1998:

a. Racial or ethnic origin
b. Political affiliations and opinions
c. Religious or other beliefs of a similar nature
d. Trade union membership
e. Physical or mental health or condition
f. Sexual life
g. Offences (including alleged offences)
h. Criminal proceedings, outcomes and sentences

Data Controller
A Data Controller is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Processor
A Data Processor, in relation to personal data, is any person (other than an employee of the Data Controller) who processes personal data on behalf of the Data Controller.

Data Subject
A Data Subject is an individual who is the subject of personal information, e.g. Joe Blogs' was provided with the Finance Plan. In this statement Joe Blogs is the Data Subject.

Third Party
A Third party, in relation to personal data, is any person other than the Data Subject, the Data Controller, Data Processor or any other person authorised to process data for the Data Controller or Processor.

Privacy Notice
A Privacy Notice is the declaration of intent made by a Data Controller when they collect personal information, this should detail how the information provided to them will be processed.

Data Protection Principles
All individuals who process personal data held by our company (manual or electronic) has an obligation to comply with the 8 Principles of the Data Protection Act 1998.

Principle 1: Obtain and process personal data fairly and lawfully.
The first data protection principle requires our firm as a Data Controller to have legitimate grounds for collecting the personal data we obtain and process.

The data obtained by our firm should not be used in an unjustified manner which could cause adverse effects on Data Subjects.

To comply with the first data protection principle our firm should inform Data Subjects of the intended use of their personal data; this can be undertaken in the form of a privacy notice.

Our Privacy Notice:
Our organisation is committed to protecting the privacy of your personal information. Our company is registered with the Information Commissioners Office (ICO) and complies with the Data Protection Act 1998 and with the data protection principles set out in the Act.

Collection of Information – your consent
We may collect personal information from you if you provide if voluntarily.

If you do provide personal information to use, we will assume that you have read this Policy and have consented to us using your personal information in the ways described in this Policy and at the point where you give us your personal information.

If, after providing us with personal information, you later decide that you do not want us to use it for particular purposes, then please write to us at the appropriate address.

Reasons for Collection of your Information

In the course of our dealing with you we may collect and process certain information about you, including your name, date of birth, address, contact details (including your email address and contact telephone number), payment details (where applicable), any benefits you receive or are entitled to (including disability benefits) (where applicable), and other information about you and your property in respect of which services and products may be provided. Your personal information may be used by us, our employees, contractors or agents to:

- identify you during any communication between you and us;
- assess eligibility for services and products (whether provided by us or on our behalf);
- communicate with you to arrange the provision of such services and products;
- administer and provide such services and products;
- detect and prevent loss, fraud and other criminal activity;
- carry out credit reference checks;
- carry out market research and to help us review, develop and improve the services and products we offer; and
- contact you (in accordance with your preferences), by post, telephone, SMS, email and other electronic means with information about products, services, promotions, and offers that may be of interest to you.

In the event that we sell or buy any business or assets, we may disclose personal information held by us to the prospective seller or buyer of such business or assets. If we or substantially all of our assets are acquired by a third party, personal information held by us will be one of the transferred assets.

Your personal information may also be used by us, our employees or agents if we are under a duty to disclose or share your personal information in order to comply with any legal obligation, or in order to enforce any agreement we have with or otherwise concerning you, or to protect our rights, property or safety or those of our customers, employees or other third parties.

With whom do we share your personal information?
Third parties such as a finance lender (where applying for a finance option).
In connection with the above purposes, your personal information may be transferred to, or otherwise processed by third party service providers acting on our behalf, our agents and law enforcement authorities (including the police).

Access to Information
The Data Protection Act 1998 gives you the right to access information held about you. You have the right to ask for a copy of the personal information held about you. You also have the right to ask for inaccuracies in information to be corrected. Any access request may be subject to a fee of £10 to meet our costs. A copy of the

information held about you by us can be requested by writing to us at the address shown.

Transfer of Information Abroad

We will not transfer your personal information outside the EU without first obtaining your consent.

Change of Policy

We may occasionally change the Privacy Policy to reflect customer and company feedback. Any changes will be shown on this page.

Dealing with Data Protection Complaints

We aim to comply fully with our obligations under the Data Protection Act (DPA) 1998. If a customer has any questions or concerns regarding our company's management of personal data including their right to access data about themselves, then they should contact the director who is responsible for ensuring our company is compliant with the DPA.

If our company holds inaccurate information, then the customer should write to our firm at the address shown providing the director with any evidence to show what the information should say keeping copies of the correspondence. If after a reasonable amount of time (28 days is recommended) the information has not been corrected, then the customer can make a complaint.

There are two courses of action:

1. Contact the director to process the complaint.
2. If the customer is still dissatisfied, they can go directly to the Information Commissioner, the independent body that overseas the DPA. They can be contacted on 0303 123 1113 or their website is www.ico.org.uk.

Principle 2: **Obtain and process personal data only for one or more specified and lawful purpose or purposes.**
Before obtaining personal data our firm must understand why it is collecting the data and be clear about the reasons for the data collection.

On collecting the data our firm should provide a clear and explanative privacy notice informing data subjects of the intended use of their data.

Our Information and Compliance Officer is to be informed to all new forms of processing at the office. There is a legal obligation under the Act to ensure all processing undertaken by a Data Controller is reflected in their Notification to the ICO (Information Commissioner's Office).

Principle 3: Personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
The amount of personal data held on a Data Subject should not exceed the amount required to suffice its purpose. Therefore, our firm should not continue to hold data on an individual when it serves no purpose.

Principle 4: Personal data should be accurate and, where necessary, kept up to date.
Our firm should take steps to ensure the personal data it holds is accurate; it should also ensure that a clear record is kept noting the origins of the data, e.g. telesales, advertisement, new customer, existing customer.

All challenges made regarding the inaccuracy of data held are to be recorded, carefully considered, and rectified when and where appropriate.

Principle 5: Hold personal data for no longer than is necessary.
A regular assessment should be undertaken by our firm to review the length of time records are held.

Once personal data is no longer required by our firm it must be destroyed, in an appropriate and secure manner.

Be careful when destroying confidential information as it can lead to information being leaked. This is a breach of the Data Protection Act 1998 that can lead to disciplinary action.

Mistakes can easily happen when throwing away notes, photocopies and printed copies. Any papers we dispose of should be carefully checked for personal data.

Destroying information earlier than necessary may also be a breach of the law so it is important that we check the retention periods before destroying any records.

It is important that we stick to the following guidelines when disposing of confidential information:

- Check any paper waste that you throw away – anything that contains personal or sensitive information must be treated as confidential waste.

- Your workspace should have access to a shredder for you to place confidential waste in.

- Do not leave confidential waste bagged up in public places.

- Sensitive or personal information kept on USBs, DVDs, CDs, laptops and PCs must be destroyed by transformation service when no longer required.

- When specialist disposal is required, items for disposal must only be passed to reputable companies that we have formal contractual agreements with.

All data related to request for personal data received by our firm under the Data Protection Act 1998, should be destroyed after five years in which the request was received.

Principle 6: Process personal data in accordance with the rights of Data Subjects under the Act.
The Data Protection Act 1998 sets out a number of rights for Data Subjects which must be upheld by Data Controllers, these consist of:
• a right of access to a copy of the information comprised in their personal data;
• a right to object to processing that is likely to cause or is causing damage or distress;
• a right to prevent processing for direct marketing;
• a right to object to decisions being taken by automated means;
• a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
• a right to claim compensation for damages caused by a breach of the Act. Data Protection Procedures Revised Aug 2011

Principle 7: Take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Our firm should ensure that data security measures are organised and implemented to reduce the potential harm of any data security breach, e.g. encryption of portal storage devices.

Our firm will make available policies and procedures for all staff and suppliers and Data Processors regarding the physical and technological security measures to be undertaken by our firm to protect the personal data held by our firm.

Our firm should be prepared to respond to a breach of data security promptly and effectively.

Principle 8: Do not transfer personal data to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.
The European Economic Area consists of the following countries:
Austria Greece Netherlands
Belgium Hungary Norway
Bulgaria Iceland Poland
Cyprus Ireland Portugal
Czech Republic Italy Romania
Denmark Latvia Slovakia
Estonia Liechtenstein Slovenia
Finland Lithuania Spain
France Luxembourg Sweden
Germany Malta

The following countries outside of the EEA are considered to have an adequate level of protection in accordance with the Data Protection Act 1998.
Andorra Argentina Canada Faroe Islands
Israel Guernsey Isle of Man Jersey
Switzerland

It is extremely unlikely that we will have to transfer data outside of the United Kingdom however, Data can be transferred outside of the countries with adequate protection if a valid exception can be justified. The following exceptions are available for application:

- Consent
- Contract Performance
- Substantial public interest
- Vital Interests
- Public Registers
- Legal Claims

Code of Practice

Our firm employees and/or sub-contractors should be aware that all personal data collected, held and processed manually or electronically as part of their employment duties, are subject to the Data Protection Principles.

Employment duties may require the publishing of your name, contact details and job title, when it relates to your professional capacity at our company.

Areas of Responsibility

Our firm's correspondent with the Information Commissioner shall be the nominated person.

On a day-to-day basis, the nominated person shall review the policy when new legislation, which has an impact on personal data, is brought into force. It is the responsibility of the nominated person and all managers to ensure that their staff are aware of the company Data Protection Policy, Procedures and relevant guidance documents, as well as their personal obligations under the Data Protection Act 1998.

All members of staff and suppliers, as well as anyone processing data on behalf of our company, and other agents, have an individual responsibility not only to our firm but also to the UK Information Commissioner. Therefore, all principles set out in the Act and our firm's procedures and guidance documents must be adhered to.

Suppliers and Agents

Suppliers, Sales agents of our firm are deemed to be agents of the company and are expected to follow the procedures/guidelines set out in our Data Protection Procedures and Guidance Documents.

Vendors, Contractors, Suppliers

Our company staff must restrict access to personal data by non-employees. Access to data by Vendors, contractors and suppliers must be controlled and documented.

Vendors, contractors and suppliers must be restricted from unnecessary admittance to areas where personal data is held or processed.

Vendors, contractors and suppliers will be required to sign non-disclosure agreements as part of a contract, where access to personal data is unavoidable.

Data Security Breach
If you suspect or have proof that there has been a breach of data securities in our organisation please notify the nominated person, in the first instance. Where a breach of data has been deliberate, our firm may consider instituting disciplinary procedures against such individuals.

Notification
The Information and Compliance Officer, under the management of the nominated person, shall ensure that notification under the Data Protection Act 1998, appropriate to all aspects of our firm's business, is filed with the Office of the Information Commissioner annually. The Notification is to be annually maintained and reviewed, via an annual audit co-ordinated by the Information and Compliance Officer.

Documents should be held in accordance with Principle 5 of the Data Protection Act 1998.

Handling of sensitive & financial personal data
Explicit consent from the Data subject is required for the processing of sensitive personal data. The categories of data which have been designated as sensitive personal data under the Data Protection Act 1998 are listed in paragraph 5 of the Procedures.

Our firm also recommends that financial information be handled with the same care as sensitive personal data. For example, credit card details should be recorded separately to non-sensitive personal data and only transferred to areas of the firm that are involved in financial processing.

Similarly, staff payroll details to be disseminated via e-mail must be encrypted and should never be held on unprotected servers.

On enrolment, all contractors, suppliers, installers are asked to sign a Data Protection declaration form with a general declaration giving consent to have their data used for promotional purposes, followed by sections pertaining to references and finance.

Publishing Staff Data
It is the responsibility of all members of staff who produce material for release into the public domain (e.g. installation references) to check the level of permission granted by Data Protection Procedures.

Data Protection Training
Data Protection training will be provided as part of the initial induction training course that all members of staff are obligated to attend which will be held at our head office by the nominated person initially.

Ongoing training and external training courses will also be held and made available to everyone, and may be highlighted during individual appraisals of staff and contractors.

The frequency of training courses will be every six months.

Data Protection Policy Audit
An audit is important as it provides an assessment of whether our organisation is following good data protection practice and any staff member that holds, controls or uses personal data are bound by the Data Protection laws and need to be aware of their obligations.

An on-site audit is carried out by a Data Protection Officer who will go around the offices and questions staff members using a self-assessment checklist/audit form to enable staff to demonstrate their compliance and understanding, including the eight data protection principles.

Additionally, the Data Protection Officer will check training records and courses to understand the awareness of staff and identify potential areas where action needs to be taken.

The Officer will also check computers to see if they have password access and check how the data is backed up and see first-hand the processes for handling both electronic and manual records containing personal data.

The Data Protection Officer will provide a report with a follow up review every six months.

Non Compliance
Non-compliance matters will be resolved by informing the staff member within 24 hours of discovering the non-compliance both verbally and in writing clearly outlining the non-compliance and reasons giving the staff member a reasonable period of time to correct the issue. A face to face meeting will take place and be encouraged and if necessary it may be necessary to contact a relevant Certification Body. Our policy is always to work with the staff member to resolve the issue however if non-compliance is of such a serious nature that we cannot reach a suitable resolution then as a last resort Disciplinary Action may have to be taken.

Where applicable our firm will also notify and inform the relevant Certification Body.

Contacts and Further Information
Any queries regarding the content of these procedures should be referred to the nominated person and/or the Information and Compliance Officer.

Further information about Data Protection matters can be found on the Information Commissioner's Website at www.ico.gov.uk.

General Data Protection Regulation (GDPR)
Passed by the European Union in April of 2016, the GDPR has far reaching global impact on data security. No matter where you are based, any organisation that does business with EU citizens must comply with the GDPR's expanded and more stringent data protection rules by **May 25th, 2018.**

With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations, and to consumers and citizens. The United Kingdom will still be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public. GDPR will change the way our business can collect, use and transfer personal data.

Our firm intends to plan and prepare for the GDPR and outline the key differences between GDPR and the DPA and what areas to address across the next twelve months.

The following checklist highlights 12 steps that we are taking now to prepare for the General Data Protection Regulation (GDPR).

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), and so most of the approach to compliance will remain valid under the GDPR, however there are new elements and significant enhancements, so we will have to do things for the first time and some things differently.

1. **Awareness** – Key decision makers and key people in our organisation should be aware that the law is changing to the GDPR.
2. **Information we hold** – We should document what personal data we hold, where it came from and who we share it with.
3. **Communicating privacy information** – We should review our current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.
4. **Individuals' rights** – we should check our procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. **Subject access requests** – We should update our procedures and plan how we will handle requests within the new timescales and provide any additional information.
6. **Legal basis for processing personal data** – We should look at the various types of data processing we carry out, identify our legal basis for carrying it out and document it.
7. **Consent** – We should review how we are seeking, obtaining and recording consent and whether you need to make any changes.
8. **Children** – We should start thinking about putting systems in place to verify "individual" ages and to gather parental or guardian consent for the data processing activity.
9. **Data Breaches** – We should make sure we have the right procedures in place to detect, report and investigate a personal data breach.
10. **Data Protection by Design and Data Protection Impact Assessments** – We should familiarise ourselves now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in our organisation.

11. **Data Protection Officers** – We should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within our organisation's structure and governance arrangements.
12. **International** – If our organisation operates internationally, we should determine which data protection supervisory authority we come under.

Key GDPR areas and Mitigation Systems relevant to our business

Key GDPR Areas and Requirements	Action to be Taken	Person Undertaking the Action	Frequency of the Action
1. AWARENESS	Key decision makers are aware of the GDPR through ICO information and newsletter.	The director will oversee the implementation of the GDPR and will raise awareness of the changes that are coming and ensure staff and suppliers are trained and aware of the new procedures and policies taking place.	As and when required
2. INFORMATION WE HOLD	The personal data that we hold comes from our own customer lead generation. This data is not sold on to any other organisation but may be shared with other parties for example our lender in order to assess suitability for any of our finance options.	The director is responsible to ensure the personal data is accurate and that it is stored and used correctly. We will maintain records of personal data and processing activities and are legally liable and responsible for any breaches.	Monthly

3. COMMUNICATING PRIVACY INFORMATION	We display privacy notices in our customer facing contracts and also in our finance agreements. With regards to offering finance to customers the privacy notices have also been reviewed by the lender.	The director will ensure that when we collect personal data we give people certain information, such as our identify and how we intend to use their information and the legal basis for processing the data, our data retention periods and that individuals have a right to complain to the ICO if the think there is a problem with the way you are handling their data.	As and when required
4. INDIVIDUALS' RIGHTS	The main rights for individual under GDPR will be: Subject access; To have inaccuracies corrected; To have information erased; To prevent direct marketing; To prevent automated decision-making and profiling, and data portability.	The director will make decisions about the deletion of customer data if requested. Our systems allow us to locate and delete the data. The right to data portability is new and this is an enhanced form of subject access where we have to provide the data electronically. We accept and understand that the customer has a stronger right to have their data deleted.	As and when required

5. SUBJECT ACCESS REQUESTS	Our organisation is not anticipating handling a large number of access requests. We will not charge for complying with a request and we will have one month to comply (rather than the current 40 days).	The director will ensure that new marketing material contains additional information to people making requests, such as their data retention periods (6 years) and the right to have inaccurate data corrected.	As and when required
6. LEGAL BASIS FOR PROCESSING PERSONAL DATA	The types of data processing that we carry out and reasons are highlighted in our Privacy Notice.	Our legal basis for processing personal data is contained in or Privacy Notice which is documented here in order to comply with the GDPR's "accountability" requirements.	As and when required
7. CONSENT	Consent has to be a positive indication of agreement to personal data being processed – it cannot be inferred from silence, pre-ticked boxes or inactivity.	Our organisation must be able to demonstrate that consent was given.	As and when required
8. CHILDREN	Our firm already has systems in place for collecting individuals	This is more in line with special protection for children's personal data, particularly in the	As and when required

	ages but does not require to gather parental or guardian consent for the data processing activity in relation to its business.	context of commercial internet services such as social networking. In short, our organisation does not collect information about children – which is the UK is defined as anyone under 13.	
9. DATA BREACHES	Our firm has a procedure in place to detect, report and investigate a personal data breach. If you suspect or have proof that there has been a breach of data securities in our organisation please notify the nominated person, in the first instance. Where a breach of data has been deliberate, our firm may consider instituting disciplinary procedures against such individuals.	In some cases we would notify the individuals whose data had been subject to the breach directly, for example where the breach might leave them open to financial loss. A failure to report a breach when required could result in a fine as well as a fine for the breach itself.	As and when required
10. DATA PROTECTION BY DESIGN AND DATA PROTECTION	Guidance has been provided by ICO on	It is unlikely in our operation that a PIA will be	As and when required

IMPACT ASSESSMENTS	Privacy Impact Assessments (PIAs) and it is important to familiarise ourselves with these and implement them into our organisation. We do not always have to carry out a PIA – a PIA is required in high-risk situations.	required. The director/nominated person would be the one to conduct a DPIA (as the GDPR terms it) with other senior staff members involved. Our organisation would consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.	
11. DATA PROTECTION OFFICERS	The director and nominated person is the designated Data Protection Officer who takes responsibility for Data Protection compliance.	The firm's activities do not involve the regular and systematic monitoring of data subjects on a large scale.	As and when required
12. INTERNATIONAL	Our organisation does not operate internationally.	The GDPR contains quite complex arrangements for working out which data protection supervisory authority takes the lead when investigating a complaint with an international aspect. However, this is not relevant in our operation as all activity is conducted within	As and when required

		the UK.	

Procedure for Data Protection

FCAP020

Revision History

Version	*Revision Date*	*Revised By*	*Section Revised*
1	0	DM	22/10/2015 – Document Introduced
1.1	1	DM	10/7/2016 – Principle 5. Details of how documents should be disposed of added.
1.2	4	DM	4/2/2017 – Added "Privacy Notice" in blue to Principle 1. Added General Data Protection Regulation (GDPR) to procedure and outlined what it means to our firm. Highlighted 12 steps to take now with GDPR.
1.3	5	DM	10/3/2017 – Added how we deal with DP complaints to the "Privacy Policy".

Document Control

Document Owner:	*Managed by:*	*Approved By:*	*Date Approved:*
Security Classification:	*Next Review Date:*	*Version:*	*Department:*