G & M Direct Claim LTD

Confidentiality, Data Protection Policy and Data Security

August 19

Contents

1 INTRODUCTION

The purpose of this policy is to set out the principles that must be observed by anyone who works for G & M Direct Claim LTD and has access to person or firm identifiable information.

2 RESPONSIBILITY FOR CONFIDENTIALITY, DATA PROTECTION AND SECURITY

Ghaffar Esmailzadeh shall be responsible for:

- Oversight of compliance with this policy
- Advising staff on the application of this policy
- Approving unusual or controversial requests for disclosure of data
- Handling subject access requests
- Briefing the Board on data protection responsibilities
- Arranging for data security risk assessment
- Reviewing this policy

.

3 DUTY OF CONFIDENTIALITY

All employees working within G & M Direct Claim LTD owe a duty of confidentiality to protect all personal and firm information they come into contact with during the course of their work.

4 DATA PROTECTION

4.1 INTRODUCTION

The Data Protection Bill (Bill) was announced in the Queen's Speech on 21 June 2017. The Bill updates data protection laws in the UK, supplementing the General Data Protection Regulation (EU) 2016/679 (GDPR), implementing the EU Law Enforcement Directive, as well as extending data protection laws to areas which are not covered by the GDPR. It is intended to provide a comprehensive package to protect personal data. The Bill will replace the 1998 Act as the primary piece of data protection legislation in the UK and will come into force in May 2018.

4.2 THE DATA PROTECTION INFORMATION COMMISSIONER

The Data Protection Information Commissioner enforces and oversees the Data Protection Act. The Commissioner has a range of duties including the promotion of good information handling and the encouragement of Codes of Practice for the data controllers, that is, anyone who decides how and why personal data are processed.

The Commissioner is a UK independent supervisory authority reporting directly to the UK Parliament.

The information provided within this procedural manual is drawn from the requirements laid down by the Office of the Information Commissioner.

Further information is available from visiting the Information Commissioner's website at https://ico.org.uk/

4.3 WHY DATA IS IMPORTANT

It is essential that those that collect and use personal data to maintain the confidence of those who are asked to provide it by complying with the requirements of the Data Protection Act.

All Data Controllers must comply with the six principles that are at the heart of the Act, including the requirement to obtain and process data fairly.

4.4 INDIVIDUAL RIGHTS

Under the Act any individual concerned has a right to see almost all personal information held about them, whether it is stored on computer or in manual form. Information held by the firm must not be amended/deleted following a request to use it. In the event of receiving a so-called 'subject access request' please refer to 'Subject Access Procedures'.

4.5 ACCURACY

The Act places an obligation to ensure the accuracy of an individual's personal data. Such information should not be misleading as to any matter of fact.

4.5.1 PERSONAL OBLIGATIONS OF ALL STAFF

- All staff who deal with personal information are required to handle that information confidentially and sensitively
- Staff undertake to process personal data supplied by the firm only in accordance with the firm's instructions
- Staff obligations in respect of the Data Protection Act form part of their contract of employment

4.6 THE DATA PROTECTION PRINCIPLES

The Act sets out 6 principles, which define the obligations of the firm as a registered data user of personal data. These principles are as follows: -

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the Data Controller towards the individual.

- First data protection principle – processing must be lawful and fair;
- Second data protection principle – purposes of processing must be specified, explicit and legitimate;
- Third data protection principle – personal data must be adequate, relevant and not excessive;
- Fourth data protection principle – personal data must be accurate and kept up to date;

- Fifth data protection principle – personal data must be kept for no longer than is necessary; and
- Sixth data protection principle –personal data must be processed in a secure manner.

4.7 REQUIREMENTS OF THE PRINCIPLES

4.7.1 FIRST PRINCIPLE

'processing must be lawful and fair'

The firm must ensure that the processing is fair and lawful. Where the data is obtained from the data subject the firm must ensure that the data subject is provided with, or have made readily available to them at the time of obtaining the data: the identity of the firm the purpose for processing other necessary information as circumstances require to ensure that the processing is fair

The firm's application forms should take into account the following requirements:

- The data subject has given their consent to the processing
- The processing is necessary for the performance of a contract with the individual to which the firm and data subject is a party
- The processing is necessary to comply with legal obligations
- The processing is necessary in order to protect the vital interests of the data subject
- The processing is necessary for the administration of justice
- The processing is necessary to pursue the legitimate business interest of the firm

Firms will only need to hold or process customer's personal data for business needs for example the need to carry out a credit search in respect of an application for a loan. The customer would have been requested to sign our standard declaration in order for their consent to be provided.

4.7.2 SECOND PRINCIPLE

'purposes of processing must be specified, explicit and legitimate'

Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

4.7.3 THIRD PRINCIPLE

'personal data must be adequate, relevant and not excessive'

Personal data held for specific purposes must be more than sufficient for the purpose or purposes.

It would therefore not be sufficient to hold information on the basis that one day it may be useful, without a firm idea of how it will be used.

4.7.4 FOURTH PRINCIPLE

'personal data must be accurate and kept up to date'

All reasonable steps must be taken to ensure the accuracy of data at all times.

Firms must have controls in place to ensure that in the event of inaccurate personal data being identified procedures will exist to allow for information to be rectified, blocked or destroyed.

4.7.5 FIFTH PRINCIPLE

'personal data must be kept for no longer than is necessary'

- The firm has a document retention policy that sets out the minimum time in which documents should be retained.
- This has been formulated in line with legal and regulatory requirements.

4.7.6 SIXTH PRINCIPLE

'personal data must be processed in a secure manner

- The firm has taken measures to ensure that only authorised persons have access to personal data and these persons act only as mandated. Passwords giving access to data are frequently changed
- All reasonable steps are taken to ensure that appropriate security measures are in place to safeguard against unauthorized or unlawful processing of personal data
- All staff that has access to personal data is deemed to be reliable and training and measures have been put in place
- Staff only access and use data that is necessary to perform their job function

4.8 PROCESSING PERSONAL DATA

Processing of personal data can be broadly defined when any operation is carried out on personal data. The Act requires that personal data be processed 'fairly and lawfully'. Personal data will not be considered to be processed fairly unless certain conditions have been met.

Processing may only be carried out where one of the following conditions has been met:

- The individual has given his or her consent to the processing
- The processing is necessary for the performance of a contract with the individual
- The processing is necessary to protect the vital interests of the individual
- The process is necessary to carry out public functions

4.9 COLLECTING PERSONAL DATA

When collecting personal data it is essential that people know:

- Who you / we are
- What the data will be used for
- To whom it will be disclosed

This information can often be provided on an application form or similar document.

Data Protection wording is included within the firm's application package, which when signed by the customer provides necessary comments for processing the customer's data.

When handling, collecting, processing or storing personal data staff must ensure that:

- All personal data is both accurate and up to date
- Errors are corrected effectively and promptly
- The data is deleted/destroyed when it is no longer needed
- The personal data is kept secure at all times (protecting from unauthorized disclosure or access)

The Data Protection Act is considered when setting up new systems or when considering use of the data for a new purpose. Any changes could affect the company's existing registration with the Data Protection Registrar and an amendment to the registration sought.

It is equally important not to:

- Access personal data that you do not need for your work
- Use the data for any purpose it was not explicitly obtained for
- Keep data that would embarrass or damage the firm if disclosed (e.g. via a subject access request)
- Transfer personal data outside of the European Economic Area unless you are certain you are entitled to or consent from the individual concerned has been obtained
- Store / process / handle sensitive data unless you are certain you are entitled to or consent from the individual concerned has been obtained.

4.10 RIGHTS OF INDIVIDUALS

4.10.1 MAKE INFORMATION AVAILABLE TO INDIVIDUALS

The right to be informed covers some of the key transparency requirements of the GDPR. It is about providing people with clear and concise information about what we do with their personal data.

The controller is required to make available to the data subject a range of information, including:

- the identity and contact details of the controller and the data protection officer;
- the purpose for which their personal data is being processed;
- the existence of their right to exercise any of the below rights;
- the legal basis for the processing of their personal data; and
- the retention period or criteria used to determine the retention period.

4.10.2 RIGHT OF ACCESS

- Confirmation from the controller whether or not a data subject's personal data is being processed and, if this personal data is being processed, access to that personal data.

4.10.3 RIGHT TO RECTIFICATION

- The controller must, if requested, rectify or complete inaccurate or incomplete personal data.
- A controller must notify the competent authority (if any) from which the inaccurate personal data originated, where this personal data has been rectified.
- A controller must notify the recipients of personal data, where personal data which been rectified, which has been disclosed by the controller. Similarly the recipient must rectify the processing of the personal data in so far as they retain responsibility for it.

4.10.4 RIGHT TO ERASURE OR RESTRICTION OF PROCESSING

- The controller is obliged, if conditions are met, to erase personal data or restrict its processing without delay.
- A controller must notify the recipients of personal data, where personal data which been erased or restricted which has been disclosed by the controller. Similarly the recipient must erase or restrict the processing of the personal data in so far as they retain responsibility for it.

4.10.5 RIGHT TO RESTRICT PROCESSING

- Individuals have a right to 'block' or suppress processing of personal data.
- When processing is restricted, you are permitted to store the personal data, but not further process it.
- You can retain just enough information about the individual to ensure that the restriction is respected in future.

4.10.6 RIGHT TO DATA PORTABILITY

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services, a typical use would be in comparing alternative current accounts
- It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

- Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe.
- It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

4.10.7 RIGHT TO OBJECT

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling) – for this individuals must have an objection on "grounds relating to his or her particular situation".
- direct marketing (including profiling) - you must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.
- processing for purposes of scientific/historical research and statistics. Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

4.10.8 RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING

- A controller cannot take a significant decision based solely on automated processing unless that decision is authorised by law.

You can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

4.11 SUBJECT ACCESS REQUESTS

Clients have a right to:

- Request (a 'subject access request') details of the processing relating to them. This includes any information about themselves including information regarding the source of the data
- To have any inaccurate data corrected or removed
- In certain circumstances to stop processing likely to cause 'substantial damage or substantial distress'
- To prevent their data being used for advertising or marketing
- Not to be subject to certain 'fully automated decisions' if they significantly affect him / her

When a subject access request is received, it is important to:

- Treat the requester with courtesy and try to understand what exactly is being sought
- Act promptly and effectively as certain timescales are imposed regarding response

4.11.1 WHAT IS A SUBJECT ACCESS REQUEST?

Often a customer will not have heard of the term 'Subject Access Request'. Staff should be able to distinguish between a casual enquiry and a 'Subject Access Request'.

A Subject Access Request is not, for example, where:-

- A customer wishes to know something specific about their account, such as their balance or transaction details
- A customer wishes to raise a complaint. In these circumstances the normal complaints procedure should be followed

A Subject Access Request is where:

- A customer wishes to be provided with personal data that the firm holds about them

4.11.2 HANDLING SUBJECT ACCESS REQUESTS

It is important that subject access requests are recognised and dealt with quickly.

A subject access request may be as simple as a letter from one the firm's customers asking what information we hold about them.

If a request is received the enquirer must be sent:

- A copy of the information held on them, this includes both computer and relevant written paper records
- A description provided as to why that information is processed
- Anyone it may be seen by or passed to
- The logic involved in any automated decisions

Before any request is auctioned the Data Controller should verify the identity of the person making the request.

Subject access requests must be dealt with within one month from the date of receipt. If further details are needed from the person making the request to assist with finding the data the one month period will begin when the extra information is received.

All information sent in response to a subject access request should be easy to understand and therefore the sending of computer printouts may not be acceptable without a covering explanation on codes used.

4.11.3 IDENTIFYING THE CUSTOMER

Subject Access Requests

Firms are not obliged to comply with a subject access request until sufficient information to clearly identify the individual requesting the file has been given. Before releasing data staff should satisfy themselves as to the identity of the customer. This is important to firms, as releasing information to the wrong person is likely to amount to a breach of security.

- Any of the documents listed below may be used to identify the customer(s):
- A bank, building society or credit card statement

- A store card or catalogue statement
- A utility bill

All documents must be original, not photocopies, and dated within the last three months. It must show the customer's full name or first initial, surname and current address.

It is important that all documentation is returned to the customer once identity has been verified.

In the rare circumstances where the customer is unable to provide any of the above items, they must provide a letter confirming their identity. This must be an original, typed or headed paper, dated within the last three months and authenticated with an official stamp if applicable. This should be from an employer, solicitor or other professional body or person.

Telephone requests for information

It is important not to release any personal information to customers before you have established their identity. Requests should be treated with great care, particularly as the issues of proof of identity are difficult to manage.

The steps that need to be taken to verify the identity of the customer will depend upon the type of information, and possibly the customer.

Although wherever possible access to a data subject's personal information should be provided 'without excessive constraints or delay'. This needs to be balanced against the responsibilities of the data controller to safeguard personal information and to avoid giving personal data to another individual.

Therefore, depending on the circumstances, staff should be asking customers to confirm selective information to verify identity from the following:

Confirmation of their date of birth and postal address

Confirmation of their employment record

Confirmation of their National Insurance number

If the customer requests a Subject Access report then the customer needs to be reminded that the request needs to be put in writing, and will be dealt with in accordance with the procedures as detailed in section 4.

4.12 CREDIT REFERENCE AGENCIES

There are three major credit reference agencies in the UK at present. They are Experian, Equifax and Call Credit. Their main purpose is to supply factual information to providers of financial services in order to establish peoples credit histories.

Customers have a legal right to have access to the data held by credit reference agencies. Customers also have a right to request that the agency remove/amend incorrect data. Customers can write to the agency to obtain a copy of their credit file.

4.13 CONSENT TO OBTAIN CREDIT SEARCH

Credit searches on an individual must not be conducted without the consent of that individual. The firm's policy is to obtain this consent in writing. Staff should contact Compliance Department if they are unsure if adequate consents have been obtained.

4.14 PROCESSING FOR DIRECT MARKETING PURPOSES

To comply with the requirements of the Data Protection Act all customers both new and existing have to positively opt in to receiving advertising and marketing material from the firm.

Likewise customers have to be informed if the firm intends to pass information to a third party for marketing purposes.

Customer's personal data is collected on application forms and the election for customers not be receive marketing material is covered through the inclusion of an 'opt-in' box.

4.15 PREFERENCE SERVICES

There are a number of marketing preference services available to customers:

The Mail Preference Service (MPS)

The Telephone Preference Service (TPS)

The Fax Preference Service (FPS)

The E-mail Preference Service (EPS)

The MPS is funded by the direct mail industry to enable customers to have their names and home addresses in the UK removed from or added to lists used by the direct mail industry.

Firms must ensure that customers that have registered with the MPS do not receive any marketing material.

4.16 THIRD PARTIES AND DATA PROCESSORS

4.16.1 GENERAL GUIDELINES

- Always read the contract carefully before signing
- Check that you understand what each clause means and the effect of that clause
- Remember – a contact is an agreement enforceable in law
- Ensure that you receive a signed original of the document
- Once the contract is in force, then it is the firm's responsibility to ensure that it complies with the term of the contract

In the event of a query reference should be made to senior management

4.17 DATA PROTECTION ACT DEFINITIONS

4.17.1 DATA

Automated and manual data that is recorded as part of a relevant filing system

4.17.2 DATA CONTROLLER

The data controller is Compliance Officer/Nominated Officer

4.17.3 DATA PROTECTION COMMISSIONER

This is the name for the Data Protection Registrar

4.17.4 DATA SUBJECT

The individual who is the subject of the personal data

4.17.5 MANUAL DATA

Manual records are those which are structured by reference to individuals or criteria relating to individuals, and which allow easy access to the personal data they contain

4.17.6 NOTIFICATION

Notification by the firm of certain basic information about the data held; the purposes for which it is held; the persons to whom it may be disclosed; a general description of the technical and organisational steps a Data Controller takes to protect data held from unauthorised access, disclosure or loss; and the identity of the Data Controller i.e. Compliance is responsible for ensuring that notification / registration is completed as necessary.

4.17.7 PERSONAL DATA

This is data relating to an individual who can be identified from that data and/or other information which is the possession of or likely to come into possession of the firm

4.17.8 PROCESSING OF PERSONAL DATA

Obtaining or recording the information to be contained in the data or carrying out an operation, including disclosure by transmission / documentation, organisation, adaptation, alteration of the information or data, retrieval, blocking, erasure or destruction of the data.

4.17.9 RELEVANT FILING SYSTEMS / MANUAL DATA

Any set of information relating to individuals which is structured either by reference to individuals i.e. by name/employee code etc., or by reference to criteria i.e. age job type, credit history etc. relating to individuals so that specific information relating to an individual is readily accessible.

4.17.10 SENSITIVE DATA

Means data pertaining to: racial or ethnic origin; religions or similar beliefs; trade union membership; physical or mental health or sexual life; political options; criminal offices. This data may only be held in strictly defined situations or where explicit consent has been obtained.

4.17.11 SUBJECT ACCESS

The right of individuals to have access to the data about them and any other related information

4.17.12 THIRD PARTY

Any person other than the firm or its staff, data subject, or data processor

5 DATA SECURITY

5.1 DATA SECURITY OBLIGATIONS

Firms have a responsibility under FCA Regulations to put in place systems and controls that keep the data of customers secure whilst also minimising the risks of data loss. The nature of the steps that firms will be expected to take will depend on the size, complexity and nature of the services that the firm provides. We recommend that firms seek expert advice about both assessing their data security risks and formulating appropriate policies, as these will be unique to individual firms.

Example of policies that firms could be expected to implement in order to comply with the above include but are not limited to requirements that:

- Customer data cannot be taken off site by staff, salespeople, suppliers, IT consultants or contractors where laptops and other devices (USB sticks, CDs, hard disks etc.) are not encrypted
- Where data is taken off on site there is automatic encryption of devices or other appropriate measures
- Where customer data is transferred electronically firms use secure internet links
- Access to sensitive areas (call centres, server rooms, filing rooms) is restricted
- Staff will not be able to access data that they do not need for their roles
- Staff handling large volumes of data do not have access to internet e-mail
- Super users/staff with large amounts of access to data are monitored
- Staff data access rights are reviewed to ensure that they remain appropriate
- When staff members leave their user accounts are permanently deleted
- Paper files are locked away
- Staff dispose of hard data securely through physically destroying data e.g. by using shredders or using confidential waste bins
- There are robust password standards and that passwords are not shared

- That there are individual user accounts requiring passwords for all systems containing customer data
- Systems operate in such a way as to prohibit the setting of passwords which do not comply with password policy
- Data is securely wiped before computers are disposed or transferred to new users
- There is some mechanism to check that hard and electronic data is being destroyed competently
- Firms understand what checks are done by employment agencies it uses
- There are enhanced vetting procedures for staff with large amounts of access to customer data
- Customers' identities are authenticated using, for example, touch-tone telephone before a conversation with a call centre adviser takes place
- There are clear & consistent procedures for backing up data
- Backed up data is limited to appropriate staff
- Backup tapes are held securely
- An accurate register of laptops issued to staff is maintained
- That there is wiping of shared laptops' hard drives between uses
- Firms have security measures in place to protect data e.g. alarm systems, grilles on windows & keypad entry doors
- There is a robust policy for logging visitors in and out

5.2 DEALING WITH DATA SECURITY INCIDENTS / DATA BREACH

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

When a personal data breach has occurred, we will need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report it. However, if we decide we don't need to report the breach, we need to be able to justify this decision and we must document it.

If we determine that we need to report the data breach to the ICO then we must do so within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, then we must also inform those individuals without undue delay.