Data Protection Policy - Draft 2

Introduction

The community brokerage Network (CBN) is fully committed to compliance with the requirements of the Data Protection Act 1998.
CBN will follow procedures which aim to ensure that employees, Board members, volunteers and partners who have access to any personal data are fully aware of and abide by their duties and responsibilities under the Act.

Statement of Policy

Data for the purposes of this policy is information that is

- Automatically processed
- Recorded with the intension of being processed
- Recorded as part of a relevant filing system

To operate efficiently, CBN has to collect and use information about the people with whom it works. These may include members of the public who have used the services of an independent broker through the Community Brokerage Network (CBN), current and past brokers, board members and partners with whom it works. This information must be handled correctly, however it is collected, recorded and used, whether that be on paper, computer records or recorded by other means according to the principles within the Act.

The Principles of Data protection

The Act stipulates that anyone processing the data must comply with Eight principles of good practice, these are legally enforceable and are summarised below :

First Principle: Personal data must be processed fairly and lawfully.
There are two main conditions for meeting this principle – either that the data

subject gives consent for the data to be processed or where the processing is necessary to fulfil legal or contractual obligations. For data to be processed fairly and lawfully, the data subject should be aware of who the data controller is and why the data is being processed.

Second Principle: Personal data must only be obtained for one or more specified purpose(s) and must only be processed in a way that is consistent with the specified purpose.
Data should only be collected by data controllers where there is a specific reason for doing so. The data subject must be advised of the purpose(s) for which the data is collected and the data must not then be used for another unrelated purpose.

Third Principle: Personal data must be adequate, relevant and not excessive for the purpose it was processed for.
Only data that is needed to fulfil the purpose for which it is collected should be requested from the data subject. Data must not be collected simply because it might be useful in the future.

Fourth Principle: Personal data must be accurate and, where necessary, kept up to date.
Data controllers should take reasonable steps to check the accuracy of the information they both receive and hold. They should also ensure that data is kept up to date or, where appropriate, destroyed after a reasonable amount of time has elapsed.

Fifth Principle: Personal data processed for any purpose must not be kept longer than is necessary to fulfil that purpose.
Data controllers should not keep data for any longer than is required to fulfil the purpose for which it was collected unless there is a legal requirement to do so

Sixth Principle: Personal data must be processed in line with the data subject's rights.
Data subjects have the right:

- To access data held about them
- To prevent processing where it is likely to cause substantial damage or distress to them or anyone else
- To be informed of the logic of automated decision-making processes to which their personal data has been subjected
- To refuse to allow a data controller to use their personal data for direct marketing purposes – even if the same data controller fairly and lawfully processes their personal data for another purpose
- To request that a data controller correct or destroy data which is inaccurate. (They can only ask for data to be destroyed where there is no legal obligation on the data controller to process the data e.g. the Inland Revenue can be asked to correct inaccurate data, but they must continue to process the data to fulfil a legal obligation.)

Seventh Principle: Appropriate security measures must be taken to protect against unauthorised or illegal data processing.

Data controllers are required to ensure that adequate security controls are in

place within the workplace to protect personal data. The Office of the Information Commissioner recommends that data controllers should process data within the principles laid down in BS7799 – The British Standard on Information Security. This includes looking at password protection, physical and environmental factors surrounding both electronic and manual data storage, access and display, organisational security, staff training and security policies.

Eighth Principle: Transferring personal data outside the European Economic Area is restricted unless the rights and freedoms of data subjects are protected.

Countries out with the European Economic Area may not have the same laws protecting the privacy of the data of the individual that those within it have. Data controllers must take steps to ensure that if data is transferred out with the European Economic Area it is secure.

Personal and Sensitive Data

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal** and **sensitive personal data**

Personal data is defined as data relating to a living individual who can be identified by that data.ie could be used for fraudulent or impersonation of that person's identity

Sensitive personal data is defined as personal data consisting of information as to

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade Union membership
- Physical or Mental Health condition
- Sexual life
- Criminal proceedings or convictions

Although not stated in the Act the Information Commissioners Office will treat and include a **'financial information'** breach in the same criteria as sensitive personal data.

Handling of Personal or Sensitive Data

CBN through appropriate governance and the use of appropriate procedures and controls:

- Observe conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;

- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

These include:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information within the statutory 40 calendar days;
- The right to prevent processing in certain circumstances;
- The right to correct, rectify, block or erase information regarded as wrong information.

In addition, CBN will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a broker or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All necessary individuals are to be made fully aware of this policy and of their duties and responsibilities under the Act.

- All individuals within CBN will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that: Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which are changed periodically;
- Individual passwords should be such that they are not easily compromised.
- Allow data protection audits by CBN (if requested)

Implementation

CBN is responsible for data protection, and as such are responsible for ensuring that this Policy is implemented. Implementation will be led and monitored by the CBN Board. The CBN Board will also have overall responsibility for:

- The provision of data protection training, for CBN brokers and board members.
- The development of best practice guidelines.
- For carrying out compliance checks to ensure adherence, throughout CBN's operations, with the Data Protection Act.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. CBN will be registered as such.

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

To this end the CBN Board will be responsible for notifying and updating the Information Officer of the processing of personal data within CBN.

The CBN Board will review the Data Protection Register annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days. To this end, any changes made between reviews will be brought to the attention of the Information Officer immediately.

Updated Nov2015

Lynn Blair