DATA PROTECTION POLICY FOR PERFECT DATA SOLUTIONS LIMITED

1 POLICY STATEMENT

1.1 This is a statement of the data protection policy of Perfect Data Solutions Limited (**the Company, "we" or "us"**). This policy is designed to ensure that the Company is compliant with the Data Protection Act 1998 (**the 1998 Act**). The 1998 Act is designed to protect the use of individual's personal data and provide them with rights to access personal data held about them by organisations.

1.2 The Company is a data controller under the 1998 Act (Data Protection Registration No: Z2756934) and as such it is required to notify the Information Commissioner of what data it processes and how that data is used, before it processes any data.

1.3 The Company's Data Protection Compliance Officer is responsible for ensuring compliance with the 1998 Act and with this policy. This position is held by Neil Williams, who can be contacted on (0)208 123 9130 in the event you have any questions about data protection.

2 INFORMATION ABOUT THE COMPANY

2.1 The Company processes consumer data to facilitate credit and identity checks via its proprietary real time credit reference agency database called TrueTime and also via Equifax Limited (the **"Service"**)

2.2 Lenders who subscribes to the Service and share consumer loan data with the Company (the **"Closed User Group"** or **"CUG"**)

2.3 Consumers who make loan applications to the Closed User Group (the **"Borrowers"**).

2.4 The Company has developed a portal which allows the CUG to access shared data. The portal allows the online lenders to see, in real time:

2.4.1 full and partial applications;

2.4.2 declined applications and the reason for the decline decision;

2.4.3 approved loans and details of approved loans, including but not limited to the loan amount, the date of issue, the date of the proposed repayment and the date of actual repayment; and

2.4.4 current loan status, such as repaid in full, defaulted (including the age of default), settled, etc.

2.5 For the purpose of carrying out its business, the Company acts as both data controller and data processor of personal data. The Company primarily processes the personal data of the Borrowers to assist the CUG of the CUG with the credit worthiness assessments that they are obliged to carry out under section 55B of the Consumer Credit Act 1974 (**the 1974 Act**) and in accordance with the FCAs Responsible Lending Guidance.

2.6 As well as the Borrowers, the individuals that the Company process data about shall include employees of the Company and, potentially, employees of the CUG.

2.7 The lawful and proper treatment of all personal data by the Company is vital to the success of the Company in order to maintain the confidence of the CUG and their customers, the Borrowers. The Company recognises the importance of the data it holds and acknowledges the requirement for it to ensure that all data is carefully processed, protected and secured.

3 ACQUISITION AND USE OF PERSONAL DATA

3.1 The Company needs to collect personal data about Borrowers in order to carry out its business of providing the CUG with relevant information about Borrowers' borrowing habits.

3.2 In addition, We may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the 1998 Act.

3.3 All employees and agents of the Company have a responsibility for ensuring that We respect personal information and deal with it in a lawful and correct manner.

4 WHAT IS DATA?

4.1 In order to fall within the 1998 Act, information must first constitute 'data'. Data is information:

4.1.1 Processed by equipment operating automatically in response to instructions for that purpose (such as a computer programme), or

4.1.2 Recorded with the intention that it should be processed automatically, or

4.1.3 Recorded as part of a relevant filing system (see 4.2 below), or

4.1.4 Which, although none of the above, still forms part of an accessible record (e.g. health record, educational record, local government record).

4.2 'Relevant filing system', is defined as any set of information, which although not automatically processed, is structured either by reference to individuals, or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

5 TYPES OF DATA

5.1 There are two types of data protected under the 1998 Act: **personal data** and **sensitive personal data**.

5.1.1 Personal data is biographical information about a living individual from which that individual can be identified, such as their name and address. It also includes any expression of opinion about a person.

5.1.2 The personal data that the Company will be predominantly processing is as follows:

(a) Name; and

(b) Certain financial information, such as:

(i) When the person applied for a loan;

(ii) How much they applied for;

(iii) Whether their application was successful;

(iv) If successful, their loan status (i.e. repaid, in default, payment plan, etc);

(v) If declined, further information about the reason for the decline.

5.1.3 Sensitive personal data is information relating to a person's:

(a) Racial or ethnic origin;

(b) Political opinions;

(c) Religious or other beliefs;

(d) Trade union membership;

(e) Physical or mental health;

(f) Sexual preferences;

(g) Criminal proceedings or convictions.

5.2 There are more stringent restrictions under the 1998 Act for the processing of sensitive personal data. The only sensitive personal data the Company processes is employee data. The Company does not process the Borrowers' sensitive personal data, although staff should still be aware of what it is.

5.3 The Company recognises that whilst the Borrowers' personal data it is processing is not, under a strict interpretation of the 1998 Act, classed as sensitive personal data, given that it relates to the borrower's financial status, it is valuable and highly confidential data.

5.4 Failure to keep the data secure could have serious consequences for the Borrowers affected, including but not limited to:

5.4.1 Potential Borrowers being incorrectly turned down for loans;

5.4.2 Potential Borrowers' private financial information being released and used for criminal purposes such as fraud.

Therefore, ensuring that all data is kept secure and protected when it is processed shall be of utmost importance to the Company.

6 PROCESSING

6.1 Processing is, essentially, anything that can be done to the information. All processing must be done in accordance with the 1998 Act, which restricts how data can be processed.

6.2 Processing includes:

6.2.1 Obtaining – The data will be obtained through the CUG . The data will be sent to the Service when the borrower completes and sends an application to a member of the CUG.

6.2.2 Storing – The Borrowers' data will be securely stored on the Company's IT system and recalled each time the borrower applies for new or extended credit to a member of the CUG.

6.2.3 Holding – The data will be held on the Company's IT system. Staff of the Company and the staff of the CUG will be able to access the information.

6.2.4 Amending – The data will be live or near live data so it will be continuously and automatically amended by the Company's IT system. All updates will be stored so that the data being accessed by the CUG is current, enabling the CUG to make informed and responsible lending decisions.

6.2.5 Destroying – All data that is no longer required for the purpose or purposes of the business that is held will be completely deleted from the Service. The Company sees a clear business reason to hold data for fraud prevention purposes for a period of six years. The Company's IT system will run a daily routine to delete from the database, all data that is older than six years and clear all temporary logs capable of storing any of this data. Media holding backup data will be destroyed at six years and one month.

6.3 The above is not an exhaustive list. Most activities involving the use of personal data will be "processing" for the purposes of the 1998 Act.

7 DATA PROTECTION PRINCIPLES

7.1 All data controllers have a duty to comply with the eight data protection principles of the 1998 Act. We support fully and comply with the principles which are summarised below:

7.1.1 Personal data shall be processed fairly and lawfully. The Company shall:

(a) have legitimate grounds for collecting and using the personal data;

(b) not use the data in ways that have unjustified adverse effects on the individuals concerned;

(c) be transparent about how we intend to use the data, and ensure members of the CUG give Borrowers appropriate privacy notices when collecting their personal data;

(d) handle people's personal data only in ways they would reasonably expect; and

(e) make sure We do not do anything unlawful with the data.

7.1.2 Personal data shall be obtained for one or more of specific purpose(s) and processed in a manner compatible with that or those purpose(s). The purpose for the Company obtaining the data is to allow the CUG to comply with their duties to carry out creditworthiness checks on Borrowers under the 1974 Act and to comply with other regulatory responsibilities.

7.1.3 Personal data held must be adequate, relevant and not excessive. The data that the Company holds will be limited to information which relates directly to a Borrower's creditworthiness.

7.1.4 Personal data must be accurate and kept up to date. The purpose of the Company is to provide live, accurate and up to date data.

7.1.5 Personal data shall not be kept for longer than necessary. The data will be kept as long as is necessary for CUG to make an informed decision about a Borrower's ability to repay a loan, and in any case, not more than 6 years from the last date that the borrower makes his last repayment on a reported loan or from when they last applied for a loan.

7.1.6 Personal data shall be processed in accordance with rights of data subjects. The Company shall process all data in accordance with the 1998 Act. The Company shall particularly observe sections 158 to 160 of the 1974 Act and section 9(3) of the 1998 Act which directly relate to the disclosure to consumers of information about their financial standing held by credit reference agencies and the correction of such information where it is found to be wrong or incomplete. The Company shall also be mindful of the Borrowers'

(a) right of access to a copy of the information comprised in their personal data;

(b) right to object to processing of data that is likely to cause or is causing damage or distress;

(c) right to prevent processing for direct marketing;

(d) right to object to decisions being taken by automated means;

(e) right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and

(f) right to claim compensation for damages caused by a breach of the 1998 Act.

7.1.7 Personal data must be kept secure. The Company must, having regard to the state of technological development and the cost of implementing any measures, ensure a level of security appropriate to—

(a) the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage of the data it processes; and

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

7.1.8 Personal data shall only be transferred to a country outside the European Economic Area (**EEA**) if there is adequate protection in that country for data subjects. At this stage, the Company does not intend to transfer data outside of the EEA.

7.2 If any employee of the Company is still unsure about when and how data can be processed, for further guidance, please contact the Data Protection Compliance Officer.

8 CONSENT TO PROCESS DATA

8.1 At least **one** of the following conditions must be met in order to process personal data:

8.1.1 Consent of the data subject,

8.1.2 Necessary for the performance of a contract with the data subject,

8.1.3 Legal obligation,

8.1.4 To protect vital interests of the data subject,

8.1.5 To carry out public functions,

8.1.6 To pursue legitimate interests of the controller unless prejudicial to interests of the data subject.

8.2 In general, this should not apply to the Company with regards to data collected about Borrowers because it is not anticipated that we will be processing or storing sensitive information. However, it shall apply in relation to data collected and processed about employees (such as personnel files recording absences through illness) and so information at least **one** of the following conditions must be met in order to process sensitive personal data:

8.2.1 Explicit consent of the individual, requiring some form of positive action (such as ticking a box on a form),

8.2.2 Necessary to comply with employer's legal duties,

8.2.3 Necessary to protect vital interests of individual or another person,

8.2.4 Carried out by certain non-profit bodies,

8.2.5 The information has been made public by the individual,

8.2.6 Necessary in connection with legal proceedings, to obtain legal advice, or exercise legal rights,

8.2.7 Necessary to carry out various public functions,

8.2.8 Necessary for medical purposes (including the provision of care and treatment and the management of health care services) undertaken by a health professional or person with equivalent duty of confidentiality,

8.2.9 Necessary for equal opportunities monitoring,

8.2.10 As specified by order – Sensitive Data Order.

8.3 Consent is the most commonly relied upon condition of processing both personal and sensitive personal data. Consent to process either form of data must be informed – a data subject cannot consent to a form of processing which he is unaware would occur. This is why it is vital that the Company continues to ensure that all existing and new members of the CUG have informed their Borrowers of this additional use of their data.

8.4 The Company shall take steps to ensure the following:

8.4.1 That a sufficient data sharing agreement exists between the Company and the online lender;

8.4.2 That as part of its standard contract with all members of the CUG or third party intermediaries, brings to the attention of the Customer that their details shall be passed to the Company so that the Borrower (the data subject) has always given informed consent for the member of the CUG to process its data.

8.4.3 That the member of the CUG agrees, pursuant to section 157 of the 1974 Act, to inform the borrower of the details of the Company where it has decided not to provide the Borrower with credit as a result of information it receives from the Company.

9 EMPLOYEE DATA

9.1 As the main operation of the Company is reliant on an IT system which is able to automatically undertake the processing of the data, the employees' main role will be to monitor the IT system to ensure it is operating correctly.

9.2 The Company will process data about its employees in accordance with the Information Commissioner's Employment Practices Code. This will include regular checks to ensure that records are not irrelevant, excessive or out-of-date.

10 SUBJECT ACCESS REQUESTS

10.1 Under section 7 of the 1998 Act, any individual is entitled to copies of any data held about them by an organisation, including the data that is held by the Company. This is done by the individual making a "subject access request". A subject access request must be made in writing, so if the Company receives an oral request, we will ask for it to be put in writing. A fee of £10.00 will also be payable. If a subject access request is received, it will be passed immediately to the Data Protection Compliance Officer, who will deal with it appropriately. Providing that the request is reasonable and the information requested is under the control of the Company, the Company must respond to a subject access request within 40 days.

11 THE BORROWER'S RIGHTS UNDER SECTIONS 158 & 159 OF THE CONSUMER CREDIT ACT 1974

11.1 Upon receipt of a request in writing from a Borrower which includes prescribed information (found at Appendix 2) which is sufficient to allow the Company to identify their file and a fee of £2, the Company shall, within 7 days, give the Borrower a copy of its file.

11.2 Under section 159 of the 1974 Act, any Borrower who is given information under either section 7 of the 1998 Act or section 158 of the 1974 Act and who considers that information is incorrect, may give notice to the Company requiring it to remove or amend the incorrect information.

12 THE COMPANY'S IT SECURITY

The Company recognises it's responsibilities to protect personal data from loss, theft or misuse and takes precautions that it considers adequate to comply with those responsibilities.

13 SOCIAL NETWORKING SITES

13.1 All employees of the Company must ensure that no personal data or sensitive personal data about a fellow employee or a customer is disclosed on social networking sites. Any employee falling foul of this rule will be in breach of the 1998 Act and will be summarily dismissed by the Company on the grounds of gross misconduct.

13.2 By way of example, social networking sites include, but are not limited to, Facebook, Twitter and Google+.

14 DATA SECURITY

14.1 The Company must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Individuals may apply to the courts for compensation if they have suffered damage from such a loss.

14.2 The 1998 Act requires the Company to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

14.2.1 Confidentiality means that only people who are authorised to use the data can access it.

14.2.2 Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

14.2.3 Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore only be stored on the Company's central computer system and not on individual PCs.

14.3 Security procedures include:

14.3.1 Entry controls. Any stranger seen in entry-controlled areas should be reported.

14.3.2 Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).

14.3.3 Methods of disposal. Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

14.3.4 Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

15 ENFORCEMENT

15.1 The Information Commissioner has responsibility for enforcement of the 1998 Act throughout the UK. An individual has the right to appeal to the Information Commissioner where he or she considers that a Data Controller has not complied with its obligations under then 1998 Act.

15.2 In November 2005, the IC published a new 'Enforcement Strategy' setting out the IC's priorities for enforcement action which is to target organisations that deliberately or persistently ignore their obligations under the 1998 Act. The IC has set up a new Regulatory Action Division which will be primarily responsible for taking enforcement action which can include:

15.2.1 Criminal Prosecution (see below for Offences)

15.2.2 A caution

15.2.3 Issuing an Enforcement Notice – requiring an organisation to take specific steps to remedy non-compliance.

15.2.4 Issuing an Information Notice – requiring an organisation to supply the IC with specified information.

15.2.5 Obtaining a Search Warrant – to exercise its powers of entry and inspection where there are reasonable grounds for suspecting that a criminal offence has been committed or the DPA principles have been breached.

15.3 In addition, an individual is entitled to compensation under Section 13 of the 1998 Act where he or she has suffered damage and/or distress as a result of the Data Controllers failure to comply with the 1998 Act. This right does however have to be enforced through the Courts.

16 OFFENCES

16.1 The 1998 Act creates the following offences:

16.1.1 Processing without notification;

16.1.2 Failing to notify changes;

16.1.3 Failing to comply with an Enforcement or Information Notice;

16.1.4 False statements;

16.1.5 Obstruction of a search warrant;

16.1.6 Obtaining, disclosing, or procuring disclosure of personal data without controller's consent (i.e. allowing an external contractor to access a computer system where no right of access was given);

16.1.7 Selling, or trying to sell, personal data if that data obtained without controller's consent;

16.1.8 Enforced subject access.

17 COMPANY OBLIGATIONS

17.1 The Company will:

17.1.1 ensure that there is always one person with overall responsibility for data protection – the Data Protection Compliance Officer. Currently this position is held by Neil Williams, who can be contacted on (0)208 123 9130in the event you have any questions about data protection.

17.1.2 provide training for all staff members who handle personal information (if an employee is unsure of his or her responsibilities he or she should notify the Data Protection Compliance Officer who will consider whether further training is necessary).

17.1.3 provide clear lines of reporting and supervision for compliance with data protection.

17.1.4 carry out regular checks to monitor and assess new processing of personal data and to ensure the Company's notification to the Information Commissioner is updated to take account of any changes in processing of personal data.

18 EMPLOYEE OBLIGATIONS

18.1 All employees of the Company will, through appropriate training and responsible management:

18.1.1 observe all forms of guidance, codes of practice and procedures about the collection and use of personal information; and

18.1.2 understand fully the purposes for which the Company uses personal information; and

18.1.3 collect and process appropriate information only in accordance with the purposes for which it is to be used by the Company to meet its business needs or legal requirements; and

18.1.4 only access personal data that they require to carry out their jobs properly; and

18.1.5 ensure the information is inputted correctly into the Company's systems by following the Company's standard format (please see the example attached); and

18.1.6 ensure the information is destroyed (in accordance with the provisions of the 1998 Act) when it is no longer required; and

18.1.7 on receipt of a request from an individual for information held about them by or on behalf of the Company immediately notify the Data Protection Compliance Officer; and

18.1.8 deal with all personal information in accordance with the Company's security procedures; and

18.1.9 not send any personal information outside of the United Kingdom without the authority of Data Protection Compliance Officer.

Appendix 2

INDIVIDUALS (INCLUDING SOLE TRADERS)

YOUR RIGHTS UNDER SECTION 159 OF THE CONSUMER CREDIT ACT 1974, AND UNDER THE DATA PROTECTION ACT 1998, IF YOU THINK ANY ENTRY IN OUR FILE IS WRONG

This statement of your rights is provided by[1] together with all the information we hold about you on our files. Our postal address is [2].

Your rights are as follows–

If you think that any of the information we have sent you is wrong and that you are likely to suffer because it is wrong, you can ask us to correct it or remove it from our file.

You need to write to us telling us what you want us to do. You should explain why you think the information is wrong.

If you write to us, we have to reply in writing within 28 days.

Our reply will tell you whether we have corrected the information, removed it from our file or done nothing. If we tell you that we have corrected the information, you will get a copy.

If our reply says that we have done nothing, or if we fail to reply within 28 days, or if we correct the information but you are not happy with the correction, you can write your own note of correction and ask for it to be included on our file.

To do this, you will need to write to us within 28 days of receiving our reply. If you did not get a reply from us and you want the information we sent you to be corrected, you will need to write to us within 8 weeks of the letter you wrote to us in which you asked us to correct the information or remove it from our file.
Your letter will need to–
• include the note of correction you have written. It must not be more than 200 words long and should give a clear and accurate explanation of why you think the information is wrong. If the information is factually correct but you think it creates a misleading impression, your note of correction can explain why.
• ask us to add your note of correction to our file and to include a copy of it whenever we give anyone any of the information you think is wrong or any information based on it.

If we accept your note of correction, we have to tell you in writing within 28 days that we are going to add it to our file.
If we think it would be wrong to add your note of correction to our file, we have to apply for a ruling from the Data Protection Commissioner.

We will apply for a ruling if we do not want to include your note of correction because we think it is wrong, or because we think it is defamatory, frivolous or scandalous, or unsuitable for publication for some other reason. We can only refuse to include your note of correction if the Commissioner agrees with us.

If we have not written to you within 28 days of receiving your note of correction, or if we have written telling you that we are not going to add your note of correction to our file, you can appeal to the Data Protection Commissioner.

If you want to do this, you will have to write to the following address[3]–

The Data Protection Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone no. 01625-545700
Fax no. 01625-524510
e.mail: data@wycliffe.demon.co.uk

When you write, you must give the following details–

• your full name and address
• our name and address
• details of the information you think is wrong, including–

why you think it is wrong,
why you think you are likely to suffer because it is wrong, and
an indication of when you sent us your note of correction.

It would be helpful to the Commissioner if you could include a copy of your note of correction.

Before deciding what to do, the Commissioner may ask us for our side of the story and send us a copy of your letter. In return, you will be sent any comments we make.

The Commissioner can make any order they think fit when they have considered your appeal. For example, they can order us to accept your note of correction and add it to our file.

If at any stage we fail to correct or remove wrong information, you can ask the Data Protection Commissioner to check whether we are meeting the requirements of the Data Protection Act 1998.

The Data Protection Act 1998 requires us to take reasonable steps to check the accuracy of personal information. If you think we have failed to correct or remove wrong information about you, you have the right to ask the Data Protection Commissioner, at the above address, to check whether our dealing with your information has met this requirement.

Important Note: The various time limits referred to in this statement (mostly 28 days) start with the day following receipt and end with the day of delivery. That means (for example) that if you have 28 days to reply to a letter from us, the period starts with the day after you receive our letter; and you then have to make sure that your reply is delivered to us no later than 28 days from that date. In order to avoid the risk of losing your rights you should therefore allow for postal delays.