Data Protection Policy (Employment)

1. Introduction

At Optimum, we really do believe that it's our people who are our main competitive advantage – the 'thing' that sets us apart from our competitors. To this end we want to ensure that we recruit and retain the very best people. As part of our commitment to colleagues working at Optimum, we want to ensure that we meet our regulatory and legislative obligations, including how we process the data that you submit to us or data we collect from third-parties. At Optimum, in line with our overarching company value of 'Do Right', doing the right thing isn't optional, it's simply part of our DNA.

This Policy sets out the obligations of Optimum Credit Limited (Optimum) regarding data protection and the rights of individuals, these can include customers, suppliers, business contacts, employees and other people that Optimum has a relationship with or may need to contact ('data subjects'), in respect of their personal data under the General Data Protection Regulation (Regulation).

The Regulation defines 'personal data' as any information relating to an identifiable natural person (a data subject) who can be identified (directly or indirectly) from that information. An identifiable natural person is one who can be identified, directly or indirectly, in particular, by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out in this policy must be followed at all times by Optimum, its

employees, agents, contractors, or other parties working on behalf of Optimum.

Optimum's Data Protection Officer is responsible for informing and advising Optimum and its staff on its data protection obligations, including in relation to criminal records information, and for monitoring compliance with those obligations and with Optimum's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Data Protection Officer by email at DPO@optimumcredit.co.uk

2.The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;

b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Lawful, Fair, and Transparent Data Processing

3.1 The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

c) Processing is necessary for compliance with a legal obligation to which the controller is subject;

d) Processing is necessary to protect the vital interests of the data subject or of another natural person;

e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) Processing is necessary for the purposes of the legitimate interests (including legislative and regulatory obligations – see below) pursued by Optimum, the controller, or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data.

3.2 Except where the processing is based on consent, Optimum will satisfy itself that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose) and will document the decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.

3.3 Optimum will include information about both the purposes of the processing and the lawful basis for it in its relevant privacy notice(s).

3.4 Where sensitive personal information is processed, Optimum will also identify a lawful special condition for processing that information and document it.

3.5 Where criminal offence information is processed, Optimum will identify a lawful condition for processing that information, and document it.

As mentioned above, one of Optimum's company values is 'Do Right', and we take our legislative and regulatory obligations seriously.

4. Processed for Specified, Explicit and Legitimate Purposes

4.1 Optimum collects and processes personal data; this may include personal data received directly from data subjects (e.g. contact details used when a data subject communicates with us) and data received from third parties (e.g. recruitment agencies).

4.2 Optimum only processes personal data for specific purposes, or for other purposes expressly permitted by the Regulation. The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

4.3 When determining whether Optimum's legitimate interests are the most appropriate basis for lawful processing, we will:

a) Conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

b) If the LIA identifies a significant privacy impact, consider whether we also need to conduct a privacy impact assessment;

c) Keep the LIA under review, and repeat it if circumstances change; and

d) Include information about our legitimate interests in our relevant privacy notice(s).

5. Adequate, Relevant and Limited Data Processing

Optimum will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. Accuracy of Data and Keeping Data Up-To-Date

Optimum shall aim to ensure that all personal data collected and processed is kept accurate and up-to-date. Where any inaccurate or out-of-date data is found or advised to us, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. Timely Processing

Optimum shall not keep personal data for any longer than is necessary in consideration of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

8. Secure Processing

Optimum shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 27 and 28 of this Policy.

9. Sensitive Personal Information

9.1 Sensitive personal information is sometimes referred to as ‘special categories of personal data’ or ‘sensitive personal data’.

9.2 Optimum may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

a) We have a lawful basis for doing so, e.g. it is necessary for the performance of the employment contract, to comply with Optimum's legal and regulatory obligations or for the purposes of its legitimate interests; and

b) One of the special conditions for processing sensitive personal information applies, e.g.:

- the data subject has given explicit consent;
- the processing is necessary for the purposes of exercising the employment law rights or obligations of Optimum or the data subject;
- the processing is necessary to protect the data subject’s vital interests, and the data subject is physically incapable of giving consent;
- processing relates to personal data which are manifestly made public by the data subject;

- the processing is necessary for the establishment, exercise or defence of legal claims; or
- the processing is necessary for reasons of substantial public interest.

9.3 Before processing any sensitive personal information, colleagues must notify the Data Protection Officer of the proposed processing, in order that the Data Protection Officer may assess whether the processing complies with the criteria noted above.

9.4 Sensitive personal information will not be processed until:

a) the assessment referred to in paragraph 9.3 has taken place; and

b) the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

9.5 During the recruitment process: the HR department, with guidance from the Data Protection Officer, will ensure that (except where the law permits otherwise):

c) during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g. race, ethnic origin, or trade union membership;

d) if sensitive personal information is received, e.g. the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

e) any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

f) 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

9.6 During employment: the HR department, will process:

a) health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance, sickness absence reporting and facilitating employment-related health and sickness benefits;

b) sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting; and

c) trade union membership information for the purposes of staff administration and administering 'check off'.

10. Criminal Records Information

Criminal records information will be processed in accordance with Optimum's Criminal Records Information Policy.

11. Privacy Notices

Optimum will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes. We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

12. Individual Obligations

12.1 Individuals are responsible for helping Optimum keep their personal information up to date. You should let the HR department know if the information you have provided to Optimum changes, for example if you move house or change details of the bank or building society account to which you are paid.

12.2 You may have access to the personal information of other members of staff, suppliers, third parties and customers of Optimum in the course of your employment or engagement. If so, Optimum expects you to help meet its data protection obligations to those individuals.

12.3 If you have access to personal information, you must:

a) only access the personal information that you have authority to access, and only for authorised purposes;

b) only allow other Optimum colleagues to access personal information if they have appropriate authorisation;

c) only allow individuals who are not Optimum employees to access personal information if you have specific authority to do so;

d) keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in Optimum's Information Security Policy);

e) not remove personal information, or devices containing personal information (or which can be used to access it), from the Optimum’s premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

f) not store personal information on local drives or on personal devices that are used for work purposes.

12.4 You should contact the Data Protection Officer if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

a) processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 9.2(b) being met;

b) any data breach as set out below;

c) access to personal information without the proper authorisation;

d) personal information not kept or deleted securely;

e) removal of personal information, or devices containing personal information (or which can be used to access it), from Optimum's premises without appropriate security measures being in place; or

f) any other breach of this policy or of any of the data protection principles set out above.

13. Information Security

13.1 Optimum will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

a) Making sure that, where possible, personal information is pseudonymised or encrypted;

b) Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) Ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing e.g. pen testing, clear desk audits etc.

e) Where Optimum uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on Optimum's written instructions;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with Optimum's prior consent and under a written contract;
- the organisation will assist Optimum in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will assist Optimum in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to Optimum as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide Optimum with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell Optimum immediately if it is asked to do something infringing data protection law.

f) Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Data Protection Officer.

14. Accountability

14.1 Optimum's Data Protection Officer is to monitor compliance with the Regulation and other Data Protection Laws.

14.2 Optimum shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The name and details of the company, its Data Protection Officer, and any applicable third-party data controllers;

b) The purposes for which the company processes personal data;

c) Details of the categories of personal data collected, held, and processed by the company; and the categories of data subject to which that personal data relates;

d) Details (and categories) of any third parties that will receive personal data from the company;

e) Details of any transfers of personal data to non-EEA countries will be encrypted;

f) Details of how long personal data will be retained by the company; and

g) Detailed descriptions of all technical and organisational measures taken by the company to ensure the security of personal data.

15. Privacy Impact Assessments

Optimum shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Data Protection Officer and shall address the following areas of importance:

a) The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

b) Details of the legitimate interests being pursued by the company;

c) An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

d) An assessment of the risks posed to individual data subjects; and

e) Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

16.The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

a) The right to be informed about how, why and on what basis that information is processed - see Optimum's Privacy Notices;

b) The right of access to information about you;

c) The right to rectification - to have data corrected if it is inaccurate or incomplete;

d) The right to erasure (also known as the 'right to be forgotten') - to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing;

e) The right to restrict processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where Optimum no longer needs the personal information but you require the data to establish, exercise or defend a legal claim;

f) The right to data portability;

g) The right to object to processing (Optimum may consider whether it has legitimate grounds override your interests); and

h) Rights with respect to automated decision-making and profiling.

17. Keeping Data Subjects Informed

17.1 Optimum shall ensure that the following information is provided to every data subject when personal data is collected:

a) Identity and contact details for Optimum and the Data Protection Officer;

b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 26 of this Policy) and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which Optimum is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the 'EEA'), details of that transfer, including but not limited to the safeguards in place (see Part 29 of this Policy for further details concerning such third country data transfers);

g) Details of the length of time the personal data will be held by Optimum (or, where there is no predetermined period, details of how that length of time will be determined);

h) Details of the data subject's rights under the Regulation;

i) Details of the data subject's right, where given, to withdraw their consent to Optimum's processing of their personal data at any time;

j) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

k) Where applicable, details of any legal or contractual requirement or obligation necessitating the

collection and processing of the personal data and details of any consequences of failing to provide it; and

l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

17.2 The information set out above in Part 17.1 shall be provided to the data subject at the following applicable time:

17.2.1 Where the personal data is obtained from the data subject directly, at the time of collection;

17.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

a) If the personal data is used to communicate with the data subject, at the time of the first communication;

b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or

c) In any event, not more than one month after the time at which Optimum obtains the personal data.

18. Data Subject Access

18.1 A data subject may make a subject access request ('SAR') at any time to find out more about the personal data which Optimum holds about them. Optimum is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

18.2 All subject access requests received must be notified to the Data Protection Officer.

18.3 Optimum does not charge a fee for the handling of normal SARs. Optimum reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

19. Rectification of Personal Data

19.1 If a data subject informs Optimum that personal data held by the company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

19.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

20. Erasure of Personal Data

20.1 Data subjects may request that Optimum erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for Optimum to hold that personal data with respect to the purpose for which it was originally collected or processed;

b) The data subject wishes to withdraw their consent to Optimum holding and processing their personal data;

c) The data subject objects to Optimum holding and processing their personal data (and there is no overriding legitimate interest to allow Optimum to continue doing so) (see Part 23 of this Policy for further details concerning data subjects' rights to object);

d) The personal data has been processed unlawfully; or

e) The personal data needs to be erased in order for Optimum to comply with a particular legal obligation.

20.2 Unless Optimum has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

20.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

21. Restriction of Personal Data Processing

21.1 Data subjects may request that Optimum ceases processing the personal data it holds about them. If a data subject makes such a request, Optimum shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

21.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

22. Data Portability

22.1 Optimum processes personal data using automated means.

22.2 Where data subjects have given their consent to Optimum to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between Optimum and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers,

e.g. other organisations).

22.3 To facilitate the right of data portability, Optimum shall make available all applicable personal data to data subjects in the following industry format(s):

a) JSON; or

b) XML

22.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.

22.5 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

23. Objections to Personal Data Processing

23.1 Data subjects have the right to object to Optimum processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for statistics purposes.

23.2 Where a data subject objects to Optimum processing their personal data based on its legitimate interests, Optimum shall cease such processing forthwith, unless it can be demonstrated that Optimum legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

23.3 Where a data subject objects to Optimum processing their personal data for direct marketing purposes, Optimum shall cease such processing forthwith.

24. Automated Decision-Making

24.1 In the event that Optimum uses personal data for the purposes of automated decision- making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from Optimum.

24.2 The right described in Part 24.1 does not apply in the following circumstances:

a) The decision is necessary for the entry into, or performance of, a contract between Optimum and the data subject;

b) The decision is authorised by law; or

c) The data subject has given their explicit consent.

25. Profiling

Where Optimum uses personal data for profiling purposes, the following shall apply:

a) Clear information explaining the profiling will be provided, including its significance and the likely consequences;

b) Appropriate mathematical or statistical procedures will be used;

c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and

d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 27 and 28 of this Policy for more details on data security).

26. Personal Data

Personal data is defined as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and 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 is defined as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; trade union membership; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Optimum only holds personal data that is directly relevant to its dealings with a given data subject. That data will be collected, held, and processed in accordance with the data protection principles and with this policy.

27. Data Protection Measures

Optimum shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a) Never put personal or confidential data in the body of an email, or in an attachment, unless encrypted and the encryption pass-phrase is communicated through a different route;

b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely;

c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is

reasonably practicable;

e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

f) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

g) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient e.g. via Royal Mail or special delivery services;

h) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

i) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

j) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;

k) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to Optimum or otherwise;

l) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Optimum where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to Optimum that all suitable technical and organisational measures have been taken);

m) All personal data stored electronically will be backed up as documented in the Business Continuity Plan;

n) All electronic copies of personal data should be stored securely;

o) All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols; and

p) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Optimum, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

28. Organisational Measures

Optimum shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All employees, agents, contractors, or other parties working on behalf of the Optimum shall be made fully aware of both their individual responsibilities and Optimum’s responsibilities under the

Regulation and under this Policy, and shall be provided with a copy of this Policy;

b) Only employees, agents, sub-contractors, or other parties working on behalf of Optimum that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by Optimum;

c) All employees, agents, contractors , or other parties working on behalf of Optimum handling personal data will be appropriately trained to do so;

d) All employees, agents, contractors, or other parties working on behalf of the Optimum handling personal data will be appropriately supervised;

e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f) The performance of those employees, agents, contractors, or other parties working on behalf of Optimum handling personal data shall be regularly evaluated and reviewed;

g) All employees, agents, contractors, or other parties working on behalf of Optimum handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

h) All agents, contractors, or other parties working on behalf of Optimum handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Optimum arising out of this Policy and the Regulation; and

i) Where any agent, contractor or other party working on behalf of Optimum handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Optimum against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

29. Transferring Personal Data to a Country Outside the EEA

29.1 In the event that Optimum transfer (‘transfer’ includes making available remotely) personal data to countries outside of the EEA.

29.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner’s Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

c) The transfer is made with the informed consent of the relevant data subject(s);

d) The transfer is necessary for the performance of a contract between the data subject and Optimum (or for pre-contractual steps taken at the request of the data subject);

e) The transfer is necessary for important public interest reasons;

f) The transfer is necessary for the conduct of legal claims;

g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

30. Data Breach Notification

30.1 A data breach may take many different forms, for example:

a) loss or theft of data or equipment on which personal information is stored;

b) unauthorised access to or use of personal information either by a colleague or third party;

c) loss of data resulting from an equipment or systems (including hardware and software) failure;

d) human error, such as accidental deletion or alteration of data;

e) unforeseen circumstances, such as a fire or flood;

f) deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

g) ‘blagging’ offences, where information is obtained by deception.

30.2 All personal data breaches must be reported immediately to Optimum’s Data Protection Officer.

30.3 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage).

30.4 The Data Protection Officer must ensure that the Information Commissioner’s Office is informed of the breach.

30.5 Without delay, and in any event, within 72 hours after having become aware of it.

30.6 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 30.3) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

30.7 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of Optimum's Data Protection Officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach; and

e) Details of the measures taken, or proposed to be taken, by Optimum to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

31. Training

Optimum will ensure that colleagues are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

32. Failure to Comply

32.1 Optimum takes compliance with this policy very seriously. Failure to comply with the policy:

a) puts at risk the individuals whose personal information is being processed;

b) carries the risk of significant civil and criminal sanctions for the individual and the Company; and

c) may, in some circumstances, amount to a criminal offence by the individual.

32.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our Disciplinary or Probation Policies, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

32.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Officer for help and advice.