Data Protection Privacy Notice (Employment)

Introduction

This notice explains what personal data (information) we hold about you, how we collect it, and how we use and may share information about you during your employment and after it ends. We are required to notify you of this information under data protection legislation.

Please ensure that you read this notice (sometimes referred to as a 'privacy notice') and any other similar notice we may provide to you from time to time when we collect or process personal information about you.

1. Who collects the information

Optimum Credit Limited (Optimum) is a 'data controller' and gathers and uses certain information about you.

2. Data protection principles

Optimum will comply with the data protection principles when gathering and using personal information, as set out in our **Data Protection Policy (Employment**), which can be found on the Company wiki. Alternatively, you can request a copy by emailing DPO@optimumcredit.co.uk.

3. About the information we collect and hold

3.1. What information

We may collect the following information during your employment:

- Your name, contact details (i.e. address, home and mobile phone numbers, email address) and emergency contacts (i.e. name, relationship and home and mobile phone numbers);
- Information collected during the recruitment process that we retain during your employment – See Data Protection Privacy Notice (Recruitment), available on the wiki;
- Employment contract information;
- Details of salary and other payments (eg bonus, overtime), benefits, bank/building society, National Insurance and tax information, your age;
- Information relating to Inland Revenue requirements (eg forms P45, P46, P11D, P60)
- Details relating to maternity, paternity, adoption, shared parental, bereavement and other types of leave or payments, as outlined in our Leave Policy, available on wiki;
- Details of your spouse/partner, any dependants, emergency contacts or nominated persons under the Life Assurance Scheme;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- A copy of your passport, birth and/or marriage certificate and driving licence;
- Where relevant, details of your share incentive arrangements, and all information included in these and necessary to implement and administer them;
- Details of your pension arrangements, and all information included in these and necessary to implement and administer them;
- Information in your sickness and absence records (including sensitive personal information regarding your physical and/or mental health, fit notes, Return to Work forms);
- Your marital status, racial or ethnic origin, gender and sexual orientation, religious or similar

beliefs;
- Criminal records information, including the results of Disclosure and Barring Service (DBS) checks;
- Information relating to regular credit and/or fraud checks (see Appendix 1)
- Information on investigations involving you;
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you;
- Details of call monitoring and/or Training & Competence records, including test and exam results;
- Details of qualifications and certificates eg CeMap, first aid, fire marshal
- Details of your appraisals and performance reviews;
- Details of your probation/performance/performance management/counselling notes/ development/ improvement plans (if any);
- Details of your time and attendance records;
- Photographs, which may also be used for internal/external communications and media/PR, and CCTV footage;
- Information in applications you make for other positions within our organisation;
- Information about your use of our IT, communication and other systems, and other monitoring information;
- Details of your use of business-related social media, such as LinkedIn;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur); and
- Information regarding your leaving the organisation including resignation letter, exit interview form, reason for leaving;
- Details in references about you that we give to others.

Certain of the categories above may not apply to you if you are a worker, agency worker, independent contractor, freelancer, volunteer, intern, on student placement or on work experience placement.

3.2. How we collect the information

We may collect this information from you, your personnel records, the Home Office, share scheme administrators, pension administrators or trustees, your doctors, from medical and occupational health professionals we engage and from our insurance benefit administrators, the relevant professional body the Disclosure and Barring Service (DBS), credit search agencies, the relevant fraud sharing database (see Appendix 1), the Department of Work & Pensions, other employees, consultants and other professionals we may engage (e.g. to advise us generally and/or in relation to any grievance, conduct appraisal or performance review procedure), systems administration including door entry system, CCTV, computer activity logs, internet browsing history, firewall logs, internet proxy logs, application logs, remote access logs, email and instant messaging platforms, telephone system, voicemail, company mobile phone records, or any other company asset issued to you as part of your role.

3.3. Why we collect the information and how we use it

We will typically collect and use this information for the following purposes (other purposes that may also apply are explained in our **Data Protection Policy (Employment)**:

- for the performance of a contract with you, or to take steps to enter into a contract;
- for compliance with a legal obligation (e.g. our obligations to you as your employer under

employment protection and health safety legislation, and under statutory codes of practice, such as those issued by ACAS); and
- for the purposes of our legitimate interests or those of a third party (such as a benefits provider), but only if these are not overridden by your interests, rights or freedoms.

Further information on the monitoring we undertake in the workplace and how we do this is available in our **Data Protection Policy (Employment)**, available on the wiki.

We seek to ensure that our information collection and processing is always proportionate. We will notify you of any material changes to information we collect or to the purposes for which we collect and process it.

3.4. How we may share the information

We may also need to share some of the above categories of personal information with other parties, such as other companies within the Optimum Credit group, recruitment/HR consultants, professional advisers, benefits and insurance providers, payroll administrators and trustees, Welsh Assembly Government, Welsh European Funding Office, The European Social Fund, The Wales Contact Centre Forum, credit search and fraud agencies (see Appendix 1), other Graduate Programme consortium members and other relevant third parties such as the Inland Revenue or with potential purchasers of some or all of our business or on a re-structuring. Where possible, information will be anonymised.

We may need to share this data for a number of reasons such as to fulfil the employment contract, provide suitable benefits, enable regular checks to be completed (eg credit checks), to ensure compliance with company policies or for internal reporting purposes, or for other legitimate business purposes. The recipient of the information will be bound by confidentiality obligations. We may also be required to share some personal information with our regulators or as required to comply with the law.

3.5. Where information may be held

Information may be held at our offices and third-party agencies, service providers, representatives and agents as described above.

3.6 How long we keep your information

We keep your information during and after your employment for no longer than is necessary for the purposes for which the personal information is processed. Further details on this are available in our Data Protection Policy (Employment) and/or our HR schedule of the Data Retention Policy available on request from DPO@optimumcredit.co.uk.

4. Your rights to correct and access your information and to ask for it to be erased

Please contact Optimum's Data Protection Officer (DPO) at DPO@optimumcredit.co.uk if (in accordance with applicable law) you would like to correct or request access to information that we hold relating to you or if you have any questions about this notice. You also have the right to ask for some, but not all, of the information we hold and process to be erased (the ‘right to be forgotten’) in certain circumstances. Our Data Protection Officer will provide you with further information about the right to be forgotten, if you ask for it.

5. Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being

accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

6. How to complain

We hope that our **Data Protection Officer** can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

APPENDIX 1 - FRAUD DATA BASES

GENERAL

1. We will check your details against the Cifas databases established for the purpose of allowing organisations to record and share data on their fraud cases, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct (“Relevant Conduct”) carried out by their staff and potential staff. “Staff” means an individual engaged as an employee, director, trainee, homeworker, consultant, contractor, temporary or agency worker, or self-employed individual, whether full or part time or for a fixed-term.
2. The personal data you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and and other Relevant Conduct and to verify your identity.
3. Details of the personal information that will be processed include: name, address, date of birth, any maiden or previous name, contact details, document references, National Insurance Number, and nationality. Where relevant, other data including employment details will also be processed.
4. We and Cifas may also enable law enforcement agencies to access and use your personal data to detect, investigate, and prevent crime.
5. We process your personal data on the basis that we have a legitimate interest in preventing fraud and other Relevant Conduct, and to verify identity, in order to protect our business and customers and to comply with laws that apply to us. This processing of your personal data is also a requirement of your engagement with us.
6. Cifas will hold your personal data for up to six years if you are considered to pose a fraud or Relevant Conduct risk.

CONSEQUENCES OF PROCESSING

1. Should our investigations identify fraud or any other Relevant Conduct by you when applying for or during the course of your engagement with us, your new engagement may be refused or your existing engagement may be terminated or other disciplinary action taken (subject to your rights under your existing contract and under employment law generally).
2. A record of any fraudulent or other Relevant Conduct by you will be retained by Cifas and may result in others refusing to employ you. If you have any questions about this, please contact us using the details provided.

DATA TRANSFERS

1. Should Cifas decide to transfer your personal data outside of the European Economic Area, they will impose contractual obligations on the recipients of that data to protect your personal data to the standard required in the European Economic Area. They may also require the recipient to subscribe to ‘international frameworks’ intended to enable secure data sharing.

YOUR RIGHTS

1. Your personal data is protected by legal rights, which include your rights to object to our processing of your personal data, request that your personal data is erased or corrected, and request access to your personal data.
2. For more information or to exercise your data protection rights please, please contact us using the contact details provided.
3. You also have a right to complain to the Information Commissioner’s Office which regulates the processing of personal data.