Job Applicant Privacy Notice

Effective from May 2018

one Savings Bank

Contents

1. Introduction

Information that is used by OneSavings Banks plc (the "Bank") and which relates to identifiable individuals (be they employees, clients, customers or suppliers) is subject to data protection laws, most notably, the General Data Protection Regulation and the Data Protection Act 2018. This notice relates to the Bank's processing of personal data of job applicants ("Applicants")

It sets out the rights that Applicants have in respect to their personal data and explains what personal data the Bank processes, how it uses it and who it may share it with.

2. Who collects the information

For the purposes of data protection law, OneSavings Bank plc is the "controller" of the personal data of Applicants which it processes, which means that it is responsible for the data.

OneSavings Bank plc is a public limited company registered in England and Wales with registration number 07312896. It is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. It is also known as Kent Reliance, Kent Reliance Property Loans, Reliance Property Loans, Heritable Development Finance, Interbay Finance, Kent Reliable Banking Services, Prestige Finance, Jersey Home Loans Limited, Guernsey Home Loans Limited and 5D Finance Limited.

Where applicable, information is also processed by Kent Reliance Provident Society. Kent Reliance Provident Society Limited is an industrial and provident society registered in England and Wales (registered with number 31056R) and whose registered office is Reliance House, Sun Pier, Chatham, Kent ME4 4ET.

The contact details of the Bank are:

Address: Reliance House, Sun Pier, Chatham, Kent ME4 4ET

Email address: mail@osb.co.uk

Telephone number: 01634 848944

The Bank's Group Data Protection Officer is David Morgan, who can be contacted on:

Address: OSB House, Quayside, Chatham, Kent, ME4 4QZ

Email address: daaprotection@osb.co.uk

3. Definitions

It is important that you understand certain definitions used in this notice.

"**Processing**" is broadly defined and includes: obtaining, recording, holding, using, organising, altering, retrieving, disclosing, erasing or destroying personal information.

"**Personal data**" is any information relating to an identified or identifiable natural person (the "data subject").

"**Sensitive personal data**" or "special category data" is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. What information the bank collects

The Bank may collect various types of information about Applicants. This includes:

- Full name;
- Home address and proof of the same;
- Contact details including email address;
- Details of previous earnings;
- Employment history information;
- Certifications, licences and other relevant authorisations to carry out a type of work;
- Education information;
- Information about relevant achievements;
- Information about relevant skills and competence levels;
- Information about relevant interests and activities;
- Information about right to work potentially including passport details or details of work permits;
- other data contained within a CV sent to the Bank.

Some information which is processed by the Bank is sensitive personal data. This includes health related information where provided by the Applicant if applicable to enable reasonable adjustments in the interview process. for the purposes of engaging with the interview process;

The Bank also sometimes processes information about criminal records, including the results of DBS checks, when it is permitted to do so by law.

Personal data will only be used for the purposes set out in this privacy notice and no other purpose.

A more comprehensive description of the information which the Bank may process, and how and why it processes it is contained in Schedule 1.

Some of the categories of information are not processed for all categories of Staff.

5. How the information is collected

Personal data may be collected by the Bank directly from the Applicant or from other sources. These other sources include:

- recruitment agencies;
- staffing agencies;
- education and training providers;
- former employers and colleagues;
- social media networks such as LinkedIn but only where the data is publicly available and the Applicant has not utilised the privacy settings offered by the network;
- reference checks providers,
- fraud prevention organisations such as CIFAS;
- when permitted by law, the Disclosure and Barring Service;
- in some cases, the Home Office in connection with right to work checks.

A more comprehensive description of the sources of the personal data processed by the Bank is contained in Schedule.

6. Why the bank processes applicants' personal data

Personal data of Applicants is processed by the Bank for the purpose of carrying out its recruitment process. This involves:

- considering job applications;
- obtaining additional information which is relevant for considering applications and making recruitment decisions;
- carrying out interviews;
- short-listing and selecting which Applicants to make an offer of employment/engagement to;
- carrying out pre-employment checks;
- entering into employment contracts (or other contracts by means of which staff are engaged);
- making preparations for new starters.

Additional data processing may be required for complying with legal requirements which apply to the Bank such as that of ensuring that its staff have a right to work and providing a safe working environment.

Therefore, the Bank needs to process the personal data of Applicants for:

- entering into and performing employment contracts (or other engagement contracts);
- complying with its legal obligations;
- pursuing its legitimate interests which relate to recruitment, such as its interest in maintaining and complying with its recruitment policies, maintaining effective recruitment and new starter procedures, and recruiting the right candidates for available roles.

A comprehensive description of the reasons why the Bank processes personal data and the relevant legal justifications for processing data under data protection law is contained in Schedule 1.

7. Ensuring that personal data is only processed in accordance with data protection laws

The Bank always seeks to ensure that it only processes personal data in accordance with data protection laws.

The Bank will, if appropriate throughout the recruitment process, consider if the information which it holds may be out-of-date and needs to be updated or deleted, and consider if there is a need to continue to hold different types of information.

The personal data which is processed should be adequate, relevant and not excessive for the purpose for which it is processed.

Any personal data stored must also be accurate and up-to-date. Inaccurate information will be deleted or amended as appropriate.

Periodic audits will be conducted to ensure that information which is inaccurate, out-of-date, inadequate, irrelevant or excessive, is updated or discarded as appropriate, unless the Bank believes there is a sound business justification for continuing to hold on to such information.

Applicants should inform the Bank as soon as possible if any of their personal information changes. The Bank will not accept responsibility for any errors in information held on Applicants unless it has been informed of the relevant changes.

8. Whom the information may be shared with

Some personal data may need to be shared with others outside the Bank. These may include:

- former employers of the Applicant;
- education and training providers;
- ecruitment and HR consultants;
- reference checking service providers, e.g. HireRight
- providers of software which is used in the recruitment process, including but not limited to "Ceridian";
- health care professionals and health and safety consultants for the purpose of considering reasonable adjustments and measures required to provide a safe work environment;
- the Home Office if required for carrying out right to work checks;
- regulators such as the Prudential Regulation Authority and the Financial Conduct Authority;
- fraud prevention organisations such as CIFAS;
- legal advisors;
- prospective buyers of the Bank or its assets;
- other companies within our group of companies;
- law enforcement and safeguarding authorities such as the police.

In most cases the recipient of the information will be bound by confidentiality obligations.

A detailed description of who personal data may be shared with is contained in Schedule 1.

9. Where personal data is held - keeping it secure

Appropriate security measures will be taken to safeguard personal data against any accident, loss, destruction, damage or unauthorised or unlawful processing.
Some personal data is stored on cloud-based software "Ceridian".

This is subject to Ceridian's security systems which he Bank has reviewed and are considered to be sufficient. Other data is stored on the Bank's internal systems and is subject to the Bank's security measures and procedures.

General access to data about Applicants is limited to HR staff who manage the recruitment process and to the relevant hiring managers who are involved in the recruitment.

All paper files are stored in locked filing cabinets and only authorised personnel have access to these files. Paper files may not be removed from their normal place of storage without good reason and will only be removed from the Bank's premises in exceptional circumstances.

Personal data held on computer will be stored confidentially and will be password protected, encrypted or coded as appropriate. Only authorised staff have access to such data. The Bank has the necessary back up and data storage facilities in place to ensure that any personal data stored on its computers is not accidentally lost or destroyed.

Adequate training will be provided to ensure data security, and disciplinary action up to and including dismissal will be taken against any member of staff who processes personal data other than as described in this notice.

The Bank also has procedures in place to deal with any suspected data security breach. The Bank will notify Applicants of security breaches affecting their data when the Bank is legally required to do so.

10. Transfer of data outside the European Economic Area

The data that we collect from job applicants may be transferred to, and stored at, a destination outside the European Economic Area (the "EEA"). In particular, we have an operations centre in India and we engage a third party that may process personal data outside of the EEA in Mauritius. Job Applicant's Personal data may also be processed by Staff operating outside the EEA who works for the Bank or one of the Bank's suppliers. The Bank will take all steps reasonably necessary to ensure that personal data is treated securely and in accordance with this privacy policy.

In particular, when the Bank send personal data overseas, the Bank will make sure suitable safeguards are in place, in accordance with European data protection requirements, to protect the data. In all cases these safeguards will be one of the following:

- Sending the data to a country that's been approved by the European Commission as providing an adequate level of data protection law.
- Putting in place a contract with the recipient containing terms approved by the European Commission as providing a suitable level of protection.

11. How long the information is kept for

Personal data held by the Bank for a specific purpose will not be held for longer than is necessary to fulfil that purpose.

Personal data which is processed for the recruitment process will be deleted within 6 months after an Applicant is notified of the Bank's decision if the Applicant is unsuccessful.

The personal data of successful Applicants who accept an offer of employment with the Bank is processed by the Bank in accordance with the Bank's Privacy Notice to Staff.

A copy of the Bank's Privacy Notice to Staff can be obtained from the HR team. A copy of the notice will also be sent to Applicants to whom an offer of employment is made.

Applicants are referred to the Bank's Data Retention Policy for more information. The Data Retention Policy can be obtained from the Bank's HR team.

12. The rights of applicants as data subjects

Applicants, as data subjects, have a number of rights under data protection law in relation to the way in which their personal data is processed. A summary of these is included below.

If any Applicants wish to obtain more information about their rights as data subjects or wish to exercise their rights, they may contact Human Resources using the following contact details:

Email address: HR_Department@krbs.com

Any request will be responded to without delay and within one month from the date of the request, although this period may be extended by an additional two months where necessary. The Bank may refuse to act on requests which are manifestly unfounded or excessive.

Right	Description
Access	Every data subject has a right to access personal data held by the Bank about him or her. Where the response to such an access request would result in the disclosure of identifying information relating to a third party, the disclosure cannot be made without the consent of that third party, unless it is reasonable to disclose the data without consent.
Rectification	A data subject may require the rectification of his or her personal data if it is inaccurate
Erasure	In limited circumstances, such as when personal data is no longer required to achieve the purpose for which it was collected, a data subject may require the Bank to erase that personal data.
Restriction of processing	In certain circumstances, a data subject may require the restriction of the processing of their personal data by the Bank. This applies when, for example, the data is no longer required to achieve the purpose for which it was collected, but the data subject requires the data to be kept for the purpose of dealing with legal claims.
Data portability	In certain circumstances, a data subject can ask to receive personal data which they provided to the Bank, in a structured, commonly used and machine readable format, or to require the transfer of this data to another organisation.
Object	A data subject may object to the processing of their personal data on grounds relating to their particular situation, where the processing of such data is necessary for the purposes of the Bank's legitimate interests, unless the Bank is able to demonstrate, on balance, legitimate grounds for continuing to process personal data which override the data subject's rights or for the establishment, exercise or defence of legal claims.
Withdrawal of consent	If the Bank processes personal data on the basis of the data subject's consent, the data subject may withdraw his or her consent at any time. Although this will not affect the validity of anything done before consent is withdrawn the Bank will promptly cease the data processing to which the withdrawn consent relates. In most cases the Bank does not rely on consent as a basis for processing personal data.

The above is only a summary of the rights of data subjects. These rights are subject to various conditions and exceptions which are provided for by law. For more detailed information please contact the Group Data Protection Officer (see section 2 for contact details).

If an Applicant is unhappy with the manner in which a query or concern which they raised is dealt with by the Bank, they may contact the Information Commissioner at ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information or to make a formal complaint.

Purpose of processing	Type of information	Source of the information	Why the Bank needs the information (the legal basis of processing)	Who the data might be shared with
To carry out recruitment for roles available with the Bank.	Staff personal details, including name, home address, email address, contact details, marital status, details of previous earnings, bank account details, emergency contact details, NI number, details of dependants. This may include sensitive personal data such as Nationality, Ethnicity, Disability information, health declaration.	This is obtained directly from the Applicant or from recruitment agencies which put forward the Applicant.	To enter into and perform the employment/engagement contract. To comply with the Bank's legal obligations. The Bank also has a legitimate interest in complying with its recruitment policies, maintaining effective recruitment and new starter procedures, and recruiting the right candidates for available roles.	Recruitment advisors/consultants; Former employers; Education and training providers; HireRight or an alternative service provider for reference checking; Ceridian for data storage and systems maintenance; Legal advisors.
To verify an Applicant's right to work when required.	Passport details including nationality; work permit information.	This is obtained directly from the Applicant or may be obtained from the Home Office.	To comply with the legal requirement to ensure that staff are legally entitled to work.	The Home Office; Legal advisors.
To make reasonable adjustments when required.	Information about health and ability. This includes sensitive data.	This obtained directly from the Applicant. Information may be provided to the Bank by health care professionals and health and safety advisors which the Bank consults with for the purpose.	To comply with legal requirements to make reasonable adjustments.	Health care professional and health and safety advisors; Legal advisors.
To process documents/ correspondence received	Full name, Home address and proof of the same, Contact details including email address, Details of previous earnings, Employment history information, Certifications, licences and other relevant authorisations to carry out a type of work, Education information, Information about relevant achievements, Information about relevant skills and competence levels, Information about relevant interests and activities, Information about right to work potentially including passport details or details of work permits and other data contained within a CV sent to the Bank. This may include sensitive personal data such as Nationality, Ethnicity, Disability information, health declaration, religious or similar beliefs.	This is information obtained from potential employees and other third parties including recruitment consultants.	To enter into and perform the employment/engagement contract. To comply with the Bank's legal obligations. The Bank also has a legitimate interest in complying with its recruitment policies, maintaining effective recruitment and new starter procedures, and recruiting the right candidates for available roles. The Bank also has a legitimate interest in maintaining Staff records and good HR practices.	SD Worx (Ceridian system) BUPA Squire Patton Boggs Unum Aegon HireRight CIFAS TRG – expired Equiniti Best Companies Perspective (PIMS) Pharon