

FAIR PROCESSING NOTICE



Kensington Mortgage Company Limited (the 'Company') is a data controller that collects and processes personal data relating to its employees to manage the employment relationship. The Company is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the Company collect?

The Company collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the Company;
- the terms and conditions of your employment;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK, including a copy of your passport and any visas required to prove your right to work in the UK;
- information about any criminal record and your credit history;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence including your inclusion of a work colleague or union representative (including if you are a member of a trade union) to carry out the role of companion in those proceedings if applicable;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the Company needs to make reasonable adjustments;
- information about your car registration and the make and model of your car, to gain access to the Maidenhead Office Park and to provide regular or visitor car parking at the Ascot House office in the Maidenhead Office Park;
- biometric data used for identification purposes in the form of a photograph on building security passes to protect the Company's interests and deliver our duty of care to our employees and visitors;
- CCTV footage of the external perimeter of the Ascot House office in Maidenhead and the reception area of the Mark Lane office in London in order to protect the Company's interests and deliver our duty of care to our employees and visitors, and
- Annual 'Fit and Proper' declarations for employees in roles as required by the Company's Regulator the Financial Conduct Authority.

The Company collects information in a variety of ways. For example, data is collected through application forms or CVs; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as expression of wish forms); from correspondence with you; through interviews, meetings or other assessments; Employee Surveys or through HR self-service, Learning Management and Employee Benefits portals.

In some cases, the Company collects personal data about you from third parties, such as references supplied by former employers, information from employment background screening providers, information from credit reference agencies and information from credit and criminal records checks permitted by law.

Data is stored in a range of different places, including in your personnel e-file, in the Company's internal and externally hosted HR & Benefits management systems and in other IT systems, including the Company's communication systems.

Collecting data via optional disclosure?

In addition to the above information, but only where you choose to volunteer it, we may collect information around your gender identity, sexual orientation, ethnic origin, religion and whether you consider yourself to have a disability.

It is not mandatory for you to provide this information, and you are fully entitled to not do so. We process any volunteered data in this particular category for the purposes of monitoring and maintaining equal opportunities across our staffing profile.

You may also ask for any volunteered diversity information to be removed at any time.

Why does the Company process personal data?

The Company needs to process data to enter into an employment contract with you and to meet its obligations under this agreement. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to provide and administer benefit, pension and insurance entitlements.

In some cases, the Company needs to process data to ensure that it is complying with its legal/regulatory obligations and to manage business risk. For example, we are required to check your entitlement to work in the UK, to carry out criminal records and credit checks to ensure that you are permitted to undertake the role you have been offered, to deduct tax, to comply with health and safety laws, to enable you to take periods of leave to which you are entitled, and to consult with employee representatives if redundancies are proposed or a business transfer is to take place.

In other cases, the Company has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the Company to:

- run recruitment, performance management and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for employee and career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the Company complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- provide and administer employee benefit schemes, including the underwriting of insurance schemes, making insurance claims and providing voluntary access to flu vaccinations.
- ensure effective general HR and business administration;
- conduct employee engagement surveys,
- gain insight that can be used to inform the Company's Diversity & Inclusion agenda;
- provide training;
- provide references on request and with the consent of current or former employees;
- respond to and defend against legal claims;
- carry out adverse media screening on a quarterly basis for employees who have joined the Company since 1 January 2018; and
- maintain and promote fairness, consistency and equality in the workplace.

Where the Company relies on legitimate interests as a reason for processing data, it has considered whether those reasons fundamentally prejudice the data protection rights of employees or workers and has concluded that they do not.

Some special categories of personal data, such as information about health or medical conditions, union membership and criminal records and offences data is processed to ensure fair and consistent application of Company HR Policies and to carry out employment law obligations, such as those in relation to employees with disabilities and for health and safety purposes.

Who has access to data?

Your information will be shared internally, including with members of the HR Team, your line manager, managers in the business area in which you work, hiring managers and IT staff, staff involved with compliance functions, but only if access to the data is necessary for performance of their roles.

The Company shares your data with third parties that process data or process data on the Company's behalf in order to:

- carry out pre-employment background screening checks from third-party providers; including:
 - checks against Watchlists maintained by Law Enforcement and Regulatory Bodies;
 - validation of your identity and your right to work in the UK;
 - obtaining pre-employment references and validation of your employment history;
- completion of necessary criminal records checks via the Disclosure and Barring Service who will provide their findings back to the employee for sharing with the Company;
- complete credit reference checks using the Credit Reference Agency ('CRA'), Equifax. To do this, we will supply your personal information to Equifax and they will provide our background screening services provider (and, in turn, the Company) with information about you. This will include public information (including your entry on the electoral register), your financial history and verification of your identity and address.

The identities of the CRAs, their role also as fraud prevention agencies, the data they hold, the ways in which they use and share personal information data retention periods and your data protection rights with the CRAs are explained in more detail in the Credit Reference Agency Information Notice ("CRAIN"), a common statement developed by the 3 major CRAs. A copy of the CRAIN can be found here – <https://www.equifax.co.uk/crain/index.html> on the Equifax website.

- calculate, process and pay your salary, allowances, bonuses and employee benefits including the management of your payroll records and settlement of taxes in accordance with the employment contract and the Company's statutory obligations;
- provide and administer company benefits and voluntary well-being related initiatives;
- deliver, monitor and evidence the completion of mandatory training;
- provide access to external training courses and professional study programmes through specialist providers;
- manage your performance and to be able to provide evidence of the competence of employees as required under the Group Training & Competence Policy and the Group SMCR policies;
- facilitate the delivery of training as required to meet Company and regulatory requirements;
- comply with the Company's Physical Security Policy and deliver the Company's duty of care to employees, protect assets and information through building access restrictions, and use CCTV and deploy other security arrangements as required;
- administer the Company's Car Parking Policy;
- facilitate the analysis of responses to Employee Engagement Surveys;
- ensure that the Company's Health & Safety responsibilities are delivered and are managed effectively;
- provide a comfortable and safe working environment;
- deliver recognition and social events and activities;
- administer the Management Incentive Plan for eligible employees;
- audit the Company's financial accounts and operational application of the Company's HR operating policies, processes and procedures;
- provide a point of contact for agency and contractor temporary resources;
- provide outplacement support to employees in the unfortunate position of being declared redundant, and;
- protect its interests in relation to matters of employment law, taxation, immigration and health & safety;
- comply with official authorities' requests for information, where we are legally obliged to do so, for example, a court order, or where we are required to provide information as part of an official investigation.

The Company may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

All countries in the European Economic Area (including the UK during its transition period) have similar standards of legal protection for information about you, as well as those countries listed by the EU Commission as "Approved Countries" offering an adequacy level in the protection of personal data. We may give the information to processors in countries not on those lists which are not normally considered to have the same level of data protection as in the EEA or an Approved Country. If we do this, we will require the people with whom we share your information to protect it to at least UK standards, for example, by imposing contractual obligations on them, and auditing their data security measures.

How does the Company protect data?

The Company takes the security of your data seriously and has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is only accessed by its employees in the performance of their duties. Details of all Company policies can be found on the Company intranet.

Where the Company engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data. Those third parties are not permitted to further share that data with any other third party unless specifically required for the initial processing purpose, and in accordance with our contractual agreements.

For how long does the Company keep data?

The Company will hold your personal data for the duration of your employment. In accordance with other legal and regulatory rules, your data is further held for 6 years after the date of your employment ending, except where you are in a 'Senior Manager' or 'Certified Function' role as defined in the Company's Senior Manager Certification Regime policies or a member of the Company's board of directors where your data will be held indefinitely. Further information around retention periods for specific types of data is available in the HR Functional Data Retention Schedule.

Your rights

As a data subject, you have a number of rights. You can:

- ask the company to inform you for what purposes new data requests are being made;
- access and obtain a copy of your data on request;
- ask the Company to change incorrect or incomplete data;
- ask the Company to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the Company is relying on its legitimate interests as the legal ground for processing;
- ask the company for a machine-readable copy of any data that you have provided and where it has been processed in a wholly automatic manner;

- ask the Company to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the Company's legitimate grounds for processing data; and
- ask for any fully-automated decisions or profiling to be manually reviewed.

If you would like to exercise any of these rights, including making a subject access request, please send an e-mail request to HRQueries@kensingtonmortgages.co.uk or DPO@kensingtonmortgages.co.uk or write to the Company's Data Protection Officer using the contact details below.

Please note that in some circumstances we will be unable to cater for these rights as your personal information is necessary for the processing of your recruitment application, or for the purposes of managing your employment with us.

If you believe that the Company has not complied with your data protection rights, you can complain to the Company's Data Protection Officer or the [Information Commissioner](#) using the contact details provided below.

What if you do not provide necessary personal data?

You have some obligations under your employment contract to provide the Company with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the Company with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details must be provided to enable the Company to enter a contract of employment with you. If you do not provide other information, this will hinder the Company's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making.

What can I do if I have any questions about this notice?

If you have any questions about how your personal data is used or wish to complain, please contact:

The Data Protection Officer
Kensington Mortgages Limited
Ascot House
Maidenhead Office Park
Maidenhead
SL6 3QQ

DPO@kensingtonmortgages.co.uk

If you believe that your complaint or query has not been dealt with satisfactorily, you have a right to complain to the Information Commissioner's Office (www.ico.org.uk) whose contact details are:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate)