

Policy notice

ClearBank external candidate data policy notice

April 2023

Policy Summary	This policy sets out what personal data may be collected from external candidates, how and why ClearBank processes this data, and the rights of the data subjects.
Applicable Board Risk Appetite Statement(s)	
Scope	Any individual employed or engaged, or seeking to be employed or engaged, by ClearBank®.
Approver	
Policy Tier	
Effective Date	June 2022
Expiration Date	
Accountable Executive	Nadine Adams, Head of Human Resources
Policy Owner / Contact	David Grant, Head of Operational Risk Oversight

1 PURPOSE

OUR PRIVACY PROMISE

Your privacy is important to ClearBank® ("ClearBank®", "we", "us" and "our"). We are committed to protecting your personal data and being transparent about the personal data we hold and use and, wherever possible, giving you control over how we use your personal data, and this is reflected in our policies and procedures. This notice gives you information about how we process your personal data when you apply to work with us.

2 SCOPE

This notice applies to any individual seeking to be employed or engaged by ClearBank® ("you" and "your").

Please read this notice carefully. Among other things, it explains:

- **What personal data** we may collect about you in connection with: (i) your potential employment and/or engagement with us; and (ii) any related interaction between you and us;
- **How, and why, we process your personal data** and the lawful basis or bases by which we process your personal data together with other important information, such as how long we retain your personal data and who we share your personal data with; and
- **Your rights** in relation to the personal data we hold about you.

We may make changes to our notices and policies from time to time, including as may be necessary or prudent to reflect any changes in the ways in which we process personal data or any changes in laws. Any updates to this notice will be on our website.

This notice is intended to be communicated to you in a concise, transparent, intelligible, and easily accessible manner, but we appreciate that you may have queries or want to seek clarification as to its terms. Should you have any questions about this privacy

notice, then please email Clear.People@Clear.Bank and we will endeavour to respond to you as soon as possible.

3 POLICY REQUIREMENTS

3.1 *The Personal Data We Collect*

The type of personal data we process may include (as applicable) the following:

Categories of Data	Description of Data
Identity Data	Name, address, date of birth, age, marital status and details of dependants, spouse and/or partner, title, maiden name, gender, nationality, country of residence, biometrics and physical data, disability information, sound recordings, images and/or photographs, driving licence, birth certificate, marriage certificate, civil partnership document, national ID card, passport and other identification documentation (including utility bills, national insurance number, social security number, tax number, residence permit, payslips or other), directorship, SM & CR status, details on a business card or in an email signature, hobbies, socio-demographic details.
Contact Data	Email address (work and personal), address, telephone number (work and personal), mobile number (work and personal), next of kin and emergency contact information and other information in an email signature.
Recruitment Data	Information contained in a Curriculum Vitae (CV) or cover letter, employment history (including education details, training details, job titles, work history, employment gaps, compensation history, working hours, professional memberships and professional qualifications), interview notes and feedback, test scores, references, details of criminal record, county court judgements and background checks during your recruitment, details regarding sanctions and whether you are a politically exposed person or a family member of a politically exposed person, assessments of your fitness and propriety, copies of right to work documentation, pension and benefits information (medical and dental) and life assurance nominee details.
Financial Data	Bank account details, income, salary and pay details, tax, and national insurance information.
Correspondence Data	Information which you provide in, or we learn about you from any correspondence or communications with us or our employees or our partners and advisors.

Security Data	CCTV footage and other information obtained through electronic means such as swipe card records and photographs.
Technical Data	Type of device, unique device identifier (e.g. an IMEI number, IP, or Mac address), network information, the type of operating system and browser you use, time zone settings and other device related information.
Publicly Available Data	Details obtained from online searches or that is otherwise available in public records including identity data, socio-demographic data and details obtained from LinkedIn, Facebook, Instagram, or other social media networks.

3.2 *Sensitive Personal Data / Special Categories of Data*

- 3.2.1 We may process special categories of personal data (also known as sensitive personal data) as described in paragraph 3.8 below.
- 3.2.2 Information about why we process, and the lawful basis upon which we rely to process, the above personal data is set out in the table at paragraph 3.7 below.

3.3 *How Do We Collect Your Personal Data?*

- 3.3.1 We may collect personal data from you directly through your application and the recruitment process (i.e. through application forms, interviews, test scores (if applicable), CVs and references), the onboarding procedure and by completing forms or by corresponding with us by mail, phone, email or otherwise.
- 3.3.2 We may also obtain personal data from third parties or public sources including but not limited to the following:
- 3.3.2.1 Workable Software Limited, which provides recruitment management services to ClearBank, or any similar supplier appointed by ClearBank;
 - 3.3.2.2 employment agencies (if applicable);
 - 3.3.2.3 background check providers;
 - 3.3.2.4 former employers, business partners, referees, and educational institutions;
 - 3.3.2.5 credit reference agencies;
 - 3.3.2.6 real estate agencies and landlords;
 - 3.3.2.7 law enforcement and fraud prevention agencies;

- 3.3.2.8 regulatory and government bodies such as the Prudential Regulation Authority, Financial Conduct Authority, HM Revenue and Customs, National Crime Agency;
- 3.3.2.9 public registers;
- 3.3.2.10 third party websites, such as LinkedIn, Facebook, Instagram, or other social media networks; and
- 3.3.2.11 CCTV cameras and swipe card access systems that operate at our offices.

3.4 *The Purposes For Which We Process Your Personal Data*

- 3.4.1 We use your personal data for a number of purposes but only where the law allows us to.
- 3.4.2 Most commonly, we will process your personal data in any circumstances where such processing is necessary:
 - 3.4.2.1 to consider your application to work with us and your potential employment/engagement with us;
 - 3.4.2.2 to comply with any legal obligation (for example to check your right to work in the UK, to comply with our regulatory obligations as a regulated entity and to prevent fraud); and/or
 - 3.4.2.3 for the purposes of the legitimate interests pursued by us or a third party. These legitimate interests include the purposes identified in the table below at paragraph 3.7 but also include other commercial interests and our internal administrative purposes. Where we rely on legitimate interests as the lawful basis for processing your personal data, we will put in place appropriate safeguards to protect your personal data and to ensure that your interests or fundamental rights and freedoms are not overridden by those legitimate interests.
- 3.4.3 We may also process your personal data where we have your consent. Where we rely on consent as the lawful basis for processing your personal data, you have the right to withdraw your consent at any time and if you wish to do so, you should contact our Data Protection Officer using the contact details set out in paragraph 3.14.3 below. The withdrawal of consent does not affect the lawfulness of processing based on consent before withdrawal or the lawfulness of processing based on other lawful grounds.
- 3.4.4 On rare occasions, we may also need to process your personal data in the following circumstances:
 - 3.4.4.1 where it is necessary to protect your vital interests or those of another person; and
 - 3.4.4.2 where it is necessary for the performance of a task carried out in the public interest such as equal opportunities monitoring.

- 3.5 We may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.
- 3.6 We may process your personal data ourselves or in conjunction with our third-party service providers in accordance with paragraph 3.12.
- 3.7 Information about the purposes for which we use your personal data, the types of personal data we process to achieve these purposes and the lawful basis by which we process it, is set out in the table below:

Purpose/Activity	Type of Personal Data Processed	Lawful Basis for Processing
Recruitment <ul style="list-style-type: none"> to progress your application and make a decision about your recruitment or engagement, the verification and assessment of your ability to work for or with ClearBank®, to ensure that you are suitable for your role, interviewing you and obtaining references to determine the terms on which you work with us and draft your employment/services contract to carry out background checks and ensure you are legally entitled to work for or with ClearBank® for administration purposes 	<ul style="list-style-type: none"> Identity Data Contact Data Recruitment Data Employment Data Financial Data Correspondence Data Security Data Technical Data Publicly Available Data 	<ul style="list-style-type: none"> Consent Performance of a contract and to take steps prior to entering into a contract Compliance with a legal obligation Our legitimate interests and your legitimate interests: to operate and manage our business, recruit candidates who are able to perform the role, to maintain employment records and ensure good employment practice, comply with legal, regulatory, and corporate governance obligations Necessary for the establishment, exercise, or defence of legal claims To carry out obligations and exercise rights in employment law For reasons of substantial public interest (including preventing or detecting unlawful acts, dishonesty and fraud and equal opportunities monitoring).
Business Management and Security <ul style="list-style-type: none"> to run and manage our business including the organisation of work, personnel management, accounting and auditing to ensure the health, safety and welfare at work and comply with health and safety obligations 	<ul style="list-style-type: none"> Identity Data Contact Data Employment Data Financial Data Correspondence Data Security Data Publicly Available Data 	<ul style="list-style-type: none"> Consent Performance of a contract and to take steps prior to entering into a contract Compliance with a legal obligation Our legitimate interests and the legitimate interests of others: to monitor and protect access to our network, systems, and facilities, to run

Purpose/Activity	Type of Personal Data Processed	Lawful Basis for Processing
<ul style="list-style-type: none"> • to provide appropriate workplace adjustments • to ensure the security of our, your and other's property • to prevent fraud • to comply with our regulatory obligations as a regulated entity • the sharing of your personal data with any prospective buyer or seller of any business or assets • the processing of personal data in connection with any actual or prospective litigation, internal or regulatory investigation 		<p>and manage our business, to ensure safe working practices and good employment practice, to comply with legal, regulatory, and corporate governance obligations and to ensure our policies and practices are adhered to and that commercially sensitive information is kept confidential</p> <ul style="list-style-type: none"> • Necessary for the establishment, exercise, or defence of legal claims • To carry out obligations and exercise rights in employment law • For reasons of substantial public interest, including preventing or detecting unlawful acts, dishonesty, and fraud
Analysis and monitoring <ul style="list-style-type: none"> • to conduct data analytics studies to better understand employee hiring rates • to carry out equal opportunities monitoring • to carry out surveys and obtain feedback on our recruitment process 	<ul style="list-style-type: none"> • Identity Data • Contact Data • Recruitment Data • Employment Data • Correspondence Data • Publicly Available Data 	<ul style="list-style-type: none"> • Consent • Performance of a contract and to take steps prior to entering into a contract • Compliance with a legal obligation • Our legitimate interests: to run and manage our business including good employment practice, to comply with legal, regulatory, and corporate governance obligations and to operate, develop and improve our business • Necessary for the establishment, exercise, or defence of legal claims • To carry out obligations and exercise rights in employment law • For reasons of substantial public interest e.g. equal opportunities monitoring

3.7.1 We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

- 3.7.2 If we need to use your personal data for an unrelated purpose, we will notify you (which may be by way of an update to this notice) and we will explain the legal basis which allows us to do so.
- 3.7.3 Please note that we may process your personal data without your knowledge or consent where this is required or permitted by law.
- 3.8 *How We Use Particularly Sensitive Personal Data And Information Relating To Criminal Convictions*
 - 3.8.1 We may process special categories of personal data (also known as sensitive personal data) including the following:
 - 3.8.1.1 details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, and political opinions;
 - 3.8.1.2 trade union membership;
 - 3.8.1.3 information about your health (including any medical condition, disability, health and sickness records); and
 - 3.8.1.4 genetic and biometric data.
 - 3.8.2 We will mostly only process sensitive personal data where it is necessary for carrying out our rights and obligations under law or where we have your explicit consent to do so. Where we request your consent, we will provide you with full details of the personal data we wish to process and the reason for processing so that you can carefully consider if you wish to consent. You can withdraw your consent at any time. Please note that we may not always need your explicit consent to process your sensitive personal data and we may also process sensitive personal data where:
 - 3.8.2.1 you have made such personal data publicly known in a clear and obvious way;
 - 3.8.2.2 it is necessary for the performance of rights and obligations in the field of employment law;
 - 3.8.2.3 it is necessary to protect you or another person from harm;
 - 3.8.2.4 the processing is necessary for reasons of substantial public interest because of the law, such as equal opportunities monitoring;
 - 3.8.2.5 the processing is necessary for the establishment, exercise, or defence of legal claims; and
 - 3.8.2.6 the processing is necessary for reasons of public interest in the area of public health.
 - 3.8.3 We may in particular use your sensitive personal data in the following ways:

- 3.8.3.1 we will conduct CCTV at any office premises which will record your physical appearance and may require you to have an access pass with your photo on it, for security purposes;
 - 3.8.3.2 we will use information about your physical or mental health or disability status to ensure your health and safety at any office premises and to assess your fitness to work and to provide reasonable adjustments (where relevant);
 - 3.8.3.3 we will use information about your gender, race, ethnic origin, age or nationality to ensure meaningful equal opportunity monitoring and reporting; and
 - 3.8.3.4 to comply with our obligations as a regulated entity.
- 3.8.4 We may also process information about criminal convictions and offences where we are either required to do so (as a regulated entity) or we are otherwise legally entitled to do so in order to ensure that you are suitable for the role as part of the recruitment process. This information may be shared with financial crime prevention agencies, law enforcement agencies and regulators.

3.9 *Questions And Complaints*

- 3.9.1 We take our data protection obligations seriously. If you have any questions or complaints about this notice, or the way that we handle your personal data, we would appreciate the chance to deal with your concerns in the first instance before you approach the relevant data protection authority. Please contact us using the details provided in paragraph 4 above.
- 3.9.2 You have the right to make a complaint at any time to the relevant supervisory authority for data protection issues, which in the UK is the Information Commissioner's Office (ICO) (www.ico.org.uk).

3.10 *Automated Decision Making*

- 3.10.1 We do not envisage that any decisions will be taken about you using automated means, however, we will notify you if this position changes.

3.11 *What If You Refuse To Provide Us With Any Personal Data?*

- 3.11.1 Where we need to collect personal data by law, or under the terms of a contract we are proposing to enter into with you and you fail to provide that data when requested, we may not be able to consider you for the role you have applied for.

3.12 *Sharing Information With Third Parties*

- 3.12.1 We will not share any of your personal data with third parties except as set out in this paragraph 3.12 or otherwise notified to you or agreed between you and us from time to time. If you apply for a position on the ClearBank website, you will be sharing your personal data with Workable Software

Limited, or a similar supplier appointed by ClearBank, and that personal data will be processed in accordance with this Notice.

- 3.12.2 Details of third parties with whom we may share your personal data is listed below:
- 3.12.2.1 Workable Software Limited or any similar supplier of recruitment management services appointed by ClearBank;
 - 3.12.2.2 any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries;
 - 3.12.2.3 employment agencies;
 - 3.12.2.4 DocuSign;
 - 3.12.2.5 former employers, business partners, referees, and educational institutions;
 - 3.12.2.6 credit reference agencies;
 - 3.12.2.7 background screening service providers, to run background and criminal checks including First Advantage Europe Limited and its affiliates;
 - 3.12.2.8 programmes which provide HR employee management services to manage your personal data, carry out the recruitment process, assist in meeting legal and statutory obligations (such as equal opportunity monitoring) and for health and safety reasons;
 - 3.12.2.9 IT providers such as cloud service providers, disaster recovery management systems, storage back-up providers for ClearBank®'s critical servers, archive storage providers, cloud storage and file sharing websites;
 - 3.12.2.10 building security who maintain our access systems and CCTV systems;
 - 3.12.2.11 regulatory and government bodies such as the Prudential Regulation Authority, Financial Conduct Authority, HM Revenue and Customs, National Crime Agency and other law enforcement and fraud prevention agencies; and
 - 3.12.2.12 legal counsel and other professional advisers including accountants and auditors.
- 3.12.3 We ensure that any third party engaged by us who processes your personal data in connection with the purposes listed above has policies and procedures in place to ensure compliance with data protection laws.
- 3.12.4 Please note that some of the third parties may be located outside of the UK and the EEA. For any third parties that are based or process data outside of the UK and the EEA, we engage such third parties in accordance with paragraph 3.13 below.

- 3.12.5 We may share your personal data with third parties where we are required to do so by law or regulation (such as in connection with an investigation of fraud or other legal enquiry) or in connection with other legal proceedings (including where we believe that your actions violate applicable laws or any agreement with us) or in order to protect our rights, property, or safety of our employee, individual suppliers, customers, or others.
- 3.12.6 In the event that our business or any part of it is sold or integrated with another business, your details may be disclosed to our advisers and those of any prospective purchaser and will be passed to the new owners of the business.

3.13 *International Transfers Of Personal Data*

- 3.13.1 From time to time, it may be necessary for us to transfer your personal data internationally as required in the course of the recruitment process. However, we will not transfer your personal data outside of the UK and the EEA unless:
- 3.13.1.1 such transfer is to a country or jurisdiction which the EU Commission or the UK has approved as having an adequate level of protection;
 - 3.13.1.2 appropriate safeguards are in place in accordance with data protection laws. These safeguards include the use of standard contractual clauses or binding corporate rules; or
 - 3.13.1.3 the transfer is otherwise allowed under data protection laws (including where we have consent, the transfer is necessary for important reasons of public interest, is necessary for the establishment, exercise or defence of legal claims or is necessary for the performance of a contract with the data subject).

3.14 *Your Rights As A Data Subject*

- 3.14.1 Subject to any conditions and requirements set out in data protection laws, you may have some, or all, of the following rights in relation to the personal data we hold about you:
- 3.14.1.1 the right to request a copy of your personal data held by us;
 - 3.14.1.2 the right to correct any inaccurate or incomplete personal data held by us;
 - 3.14.1.3 the right to request that we erase personal data we hold about you;
 - 3.14.1.4 the right to request that we restrict the processing of your data;
 - 3.14.1.5 the right to have your personal data transferred to another organisation;

3.14.1.6 the right to object to certain types of processing of your personal data by us; and

3.14.1.7 the right to complain (please see paragraph 3.9 of this notice).

3.14.2 **PLEASE NOTE** that these rights are not absolute in all situations and may be subject to conditions and provisions set out in data protection laws. We cannot, therefore, guarantee that we will be able to honour any request from you in connection with the rights set out above (for example, even if you request that we delete your personal data, we may be required by law to retain some personal data for accounting and record keeping purposes or in order that we comply with our legal and regulatory obligations including our obligations under employment law).

3.14.3 For further information, or to exercise any particular right, please contact us at DataProtectionOfficer@Clear.Bank.

3.15 *Links To Third Parties*

3.15.1 We cannot be held responsible for the activities, privacy policies or levels of privacy compliance of any website or platform operated by any third party which is not engaged by ClearBank® unless stated otherwise by law. You should check the respective privacy notices before using such website or platform.

4 ROLES AND RESPONSIBILITIES

For the purposes of data protection laws, ClearBank Limited ("ClearBank®", "we", "us", "our") is the data controller of your personal data which means that we are responsible for deciding how we hold and use your personal data.

Our contact details are:

Email: DataProtectionOfficer@Clear.Bank

Telephone: 020 3111 2328

Address: ClearBank Limited
133 Houndsditch
London
EC3A 7BX

5 POLICY EXCEPTIONS

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes or if you become aware that any personal data that we hold is not accurate.

6 STORAGE AND RETENTION OF YOUR PERSONAL DATA

6.1 As a minimum, we will store your personal data for 6 months following an unsuccessful application to work for us, but for no longer than we need it including to fulfil our legal and regulatory obligations (e.g. relating to record keeping) and to exercise or defend any legal claims. If we employ or engage you, we will store your personal data for as long as your employment and/or engagement continues and then in accordance with our internal policies.

- 6.2 For as long as we do store your personal data, we follow generally accepted industry standards and maintain reasonable safeguards to attempt to ensure the security, integrity, and privacy of your personal data. We limit access to your personal data to those employees, agents, contractors and third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.